Docket No.: SEKI-001

PATENT #11

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of		
	Yutaka YASUKURA	
Serial No.	09/445,060	Group Art Unit: 2132
Confirm. No.:	9420	Examiner: Courtney D. Fields
Filed:	December 2, 1999	
For:	AUTHENTICATION CARD SYSTEM	

SUBMISSION OF ORIGINAL DOCUMENT

U.S. Patent and Trademark Office
2011 South Clark Place
Customer Window
Crystal Plaza Two, Lobby, Room 1B03
Arlington, VA 22202

Sir:

Applicant submitted with the Amendment filed on October 3, 2003 a facsimile copy of Certified English Translation of Japanese Patent Application No. 10-139563. Applicant submits herewith the original English Translation to be made part of this application file history.

Please charge any shortage in fees due in connection with the filing of this, concurrent and future replies, including extension of time fees, to Deposit Account 16-0607 and please credit any excess fees to such deposit account.

Respectfully submitted,
FLESHNER & KIM, LLP

Carl R. Wesolowski, Esq.
Registration No. 40,372
Laura L. Lee, Esq.
Registration No. 48,752

P.O. Box 221200
Chantilly, VA 20153-1200
703 502-9440 CRW/LLL:knv
Date: October 30, 2003

SPECIFICATION

TITLE OF THE INVENTION: USER AUTHENTICATION SYSTEM, USER AUTHENTICATION CARD AND USER AUTHENTICATION DEVICE

CLAIMS

Claim 1. A user authentication system comprising a registration station provided with an information acquisition device for obtaining biological individuality data for distinguishing individuality of a user, an authentication card issuing station that issues to the user a user authentication card recorded with at least a part of the biological individuality data, and an authentication access terminal provided with an authentication-card reader for reading the information of the user authentication card and an identity acquisition device for inputting biological individuality data of the user, wherein the recorded contents in the user authentication card read out by the authentication card reader are compared with the biological individuality data of the user input to the identity acquisition device to authenticate that the user is the legitimate proprietor of the user authentication card.

Claim 2. A user authentication system comprising a registration station provided with an information acquisition device for obtaining biological individuality data for distinguishing individuality of a user, an authentication card issuing station that issues to the user a user authentication card recorded with at least a part of the biological individuality data, and an authentication access terminal provided with an identity acquisition device for obtaining biological individuality data of the user and an identity information writing device for inputting the obtained biological individuality data in said user authentication card, wherein the contents of biological individuality data recorded in said user authentication card are compared with the biological individuality data of the user obtained by said identity acquisition device by using a computing function

to authenticate that the user is the legitimate proprietor of the user authentication card.

Claim 3. The user authentication system according to claim 1 or 2, comprising further at least one certification authority that is connected to said authentication access terminal through an information communication channel, wherein the certification authority holds the record of the remaining part of the biological individuality data that was obtained at the registration station but not recorded in the user authentication card, and the part of the biological individuality data missing in the user authentication card is compared in response to an inquiry from said authentication access terminal for further authentication.

Claim 4. The user authentication system according to claim 3, wherein the information exchanged through the information communication channel is encrypted.

Claim 5. The user authentication system according to claim 3 or 4, wherein the two or more said certification authorities dividedly record part of the biological individuality data obtained at the registration station but not recorded in the user authentication card, and each certification authority compares the biological individuality data of the user input at the authentication access terminal with the part of the biological individuality data stored in the certification authority in response to inquiry from the authentication access terminal or other certification authority for further authentication.

Claim 6. The user authentication system according to any of claims 1 through 5, wherein the certification authority is provided with a memory device for recording the biological individuality data obtained at said registration station.

Claim 7. The user authentication system according to claim 6, wherein

a memory medium recoding the biological individuality data in said certification authority can be cut off from the information communication channel of the user authentication system.

Claim 8. The user authentication system according to any of claims 1 through 7, wherein said biological individuality data is handwriting.

Claim 9. The user authentication system according to any of claims 1 through 8, wherein plural kinds of biological individuality data are registered so that different transactions can be conducted in response to the kind of the input data.

Claim 10. A user authentication card capable to be used for the user authentication system according to any of claims 1 through 9, comprising a memory medium provided with a readable memory area which stores a signal for identifying the authentication card and at least part of the biological individuality data for distinguishing the individuality of a user from others.

Claim 11. The user authentication card of claim 10, comprising further a CPU and a RAM.

Claim 12. The user authentication card of claim 10 or 11, wherein said memory medium is a magnetic recording medium.

Claim 13. The user authentication card of claim 10 or 11, wherein said memory medium is an IC card.

Claim 14. A user authentication device comprising an authentication-card reader for reading the information recorded in a user authentication card, an identity acquisition device for inputting biological individuality data of the user, a judgment device for judging the authenticity by comparing the biological individuality data recorded in the user authentication card read by said authentication-card reader and the biological individuality data of the user input in said identity acquisition device, and a display device for displaying a

judgment result.

Claim 15. The user authentication device, wherein said identity acquisition device has a handwritten figure acquisition function.

Claim 16. The user authentication device of claim 15 or 16 comprising further a communication device for sending at least a part of biological individuality data of a user input to the identity acquisition device to an external certification authority and receiving a judgment result of authenticity, wherein the judgment result is displayed through said display device.

.BACKGROUND OF THE INVENTION

[0001]

Technical Field of the Invention

The present invention relates to a user authentication system for execution of individual authentication in electronic information exchange, electronic commercial transaction and so on, a user authentication card and a user authentication device for use in the user authentication system.

[0002]

Related Art

The kinds of information accessible through communication networks have become extremely diverse in recent years, which range from electronic commerce such as product trading or credit to on-line medical diagnoses or individual medical records, and to perusal of registered items or the issue of certificates from public offices. The application and utilization of such information are increasing for years.

[0003]

Such personal information has something to do with individual's privacy, and it should not be often approved the use if there is not a guarantee against leaks of the information to public. To establish a more convenient

information-based society associated with advances in electronic information communication networks, there has been a demand for a highly reliable user authentication system capable of making a clear distinction between individuals.

Such a mechanism for authenticating personal identity can also be used in a lock device to prohibit entrance of unauthorized persons into a laboratory, a business office, or a house, and for an improvement in security of electronic money.

[0004]

The password has been most commonly used in authenticating user identity. The password is easy to use, but it is hard to eliminate thieves who steal the user's passwords. To prevent password thefts, the user takes care in protecting the security of password such as to use a long password, to select a password difficult to guess, or to change the password on occasion. Cryptography has also widely been used for security in communications, which encrypts communication contents to prevent others from recognizing the contents easily even when data leakage occurs.

[0005]

Nevertheless, such security measures cannot be perfect, and the password may be stolen by others through wiretapping communication, cracking the encrypted code, or stealing a look at the password. Further, the more complicated the password is, the more difficult for the user to remember. It is also essential that any complicated data can be duplicated by any means as soon as the password is stored as digital data.

[0006]

To prevent others from pretending the user and authenticate user identity securely, there has been considered another method of authenticating user identity based on information indicative of so-called biological individuality of the

user such as a fingerprint or voiceprint. However, the biological individuality data has generally a large quantity of information, and this requires extremely dense traffic flows between an authentication access terminal and a certification authority in which the user's biological information is stored. Such dense traffic flows may cause a traffic jam in a communication channel and increase of communication time, and it is hard to apply this method to practical use except for special environments. In the method, other problems also remain with the data managing place and managing method.

[0007]

Problems to be Solved by the Invention

It is therefore an object to be solved by the present invention to provide a user authentication system that can obtain a quick response while retaining a high level of security in authenticating personal identity for electronic information exchange or electronic business transaction, and a user authentication card and a user authentication device for use in the user authentication system.

[0008]

Means to Solve the Problems

In order to solve the aforementioned objects, a user authentication system of the present invention comprises a registration station provided with an information acquisition device for obtaining biological individuality data for distinguishing individuality of a user, an authentication card issuing station that issues to the user a user authentication card recorded with at least a part of the biological individuality data, and an authentication access terminal provided with an authentication-card reader for reading the information of the user authentication card and an identity acquisition device for inputting biological individuality data of the user, in which the recorded contents in the user authentication card read out by the authentication card reader are compared

with the biological individuality data of the user input to the identity acquisition device to authenticate that the user is the legitimate proprietor of the user authentication card.

[0009]

A second user authentication system of the present invention comprises a registration station provided with an information acquisition device for obtaining biological individuality data of a user, an authentication card issuing station that issues to the user a user authentication card recorded with at least a part of the biological individuality data, and an authentication access terminal provided with an identity acquisition device for obtaining biological individuality data of the user and an identity information writing device for inputting the obtained biological individuality data in the user authentication card, in which the contents of biological individuality data recorded in the user authentication card are compared with the biological individuality data of the user obtained by the identity acquisition device by using a computing function to authenticate that the user is the legitimate proprietor of the user authentication card.

[0010]

It is preferable that the user authentication of the present invention comprises further at least one certification authority that is connected to the authentication access terminal through an information communication channel, in which the user authentication card holds a part of the biological individuality data that was obtained at the registration station and the certification authority holds the record of the remaining part thereof not recorded in the user authentication card, and the part of the biological individuality data missing in the user authentication card is compared in response to an inquiry from the authentication access terminal for further authentication.

It is preferable that the information exchanged mutually through the

information communication channel is encrypted to guarantee the security.

[0011]

Moreover, it is preferable that the two or more the certification authorities dividedly record part of the biological individuality data obtained at the registration station but not recorded in the user authentication card, and each certification authority compares the biological individuality data of the user input at the authentication access terminal with the part of the biological individuality data stored in the certification authority in response to inquiry from the authentication access terminal or other certification authority for further authentication.

Further, in the user authentication system, the certification authority may be provided with a memory device for recording the biological individuality data obtained at the registration station.

It is preferable that a memory medium recoding the biological individuality data in the certification authority can be cut off from the information communication channel of the user authentication system.

Handwriting may be used as the biological individuality data.

[0012]

In the user authentication system of the invention, the user authentication card records thereon at least a part of the biological individuality data that distinguishes the individuality of a user from others, and the biological individuality data in the user authentication card are compared with the biological individuality data input by the user on the spot, so that only the true user can pass in authentication test, thereby preventing others from pretending the user.

[0013]

Not only is it too hard to reproduce the original forms of biological

individuality from its digitized data, but also others cannot duplicate the biological individuality even if they can reproduce the digitized data. This makes it possible to offer a superior level of reliability of the user authentication.

In particular, since the biological individuality data for reference are recorded in the user authentication card, the user to be authenticated can be directly confirmed with his or her identity at the authentication access terminal without inquiring the identification from the certification authority remote from the authentication access terminal. This makes it possible to reduce a great deal of time and cost spent on communication with the certification authority.

[0014]

Though the user authentication can be performed by comparing the biological individuality data for comparison recorded in the user authentication card with the biological individuality data of a user made to input from the authentication access terminal by a logical arithmetic unit provided at the authentication access terminal, the computing function such as CPU, RAM and so on may also be provided in the user authentication card, for comparing the biological individuality data obtained from a used intending to exploiting the user authentication card with input and recorded information.

A practical use of a user authentication card provided with having advanced functions such as IC card or the like permits to mitigate the load to the authentication access terminal, reduce the equipment cost, and make the system more user-friendly. Moreover, the security can be improved by preventing the authentication data from leaking outside, as the information processing is completed within the user authentication card in such a way.

[0015]

Further, in case where the certification authority connected to the authentication access terminal via the information communication channel holds

the record of the remaining part of the biological individuality data that was not recorded in the user authentication card, and the part of the biological individuality data is compared in response to an inquiry from said authentication access terminal for further authentication, as necessary information is divided and memorized, it is impossible to break through the authentication system even if biological individuality data is restored for instance from the data recoded in the authentication card, and it is also impossible to copy the data to be used for further authentication form the authentication card.

Furthermore, even if the contents of the record in the authentication card are falsified, since the information at the certification authority is maintained, others cannot pretend to be the proper user.

Even when someone succeeds to attack the certification authority, he cannot falsify the information of the user authentication card carried by the user, thus retaining the security.

It should be appreciated that, if information diffused through the information communication channel is encoded, the security can be improved, because it is difficult to decode it, even if someone steal information in the middle of the communication channel.

[0016]

In case where the biological individuality data of a user are divided and recorded among the user authentication card and two or more certification authorities, and each certification authority compares the part of the memorized biological individuality data of the in response to an inquiry from the authentication access terminal or other certification authority for further authentication, in addition to the user authentication based on the user authentication card, the reliability of the user authentication can be enhanced by obtaining gradually the used authentication of certification authorities structured

for instance hierarchically.

[0017]

In the user authentication system of the invention, pass/fail determination may be selectively made by only the authentication result obtained by the authentication access terminal based on the information recorded in the user authentication card, or for more secure determination by adding the authentication results by the certification authority or authorities based on the information held in the authority or authorities but not recorded in the user authentication card, according to the grade of the required reliability of the authentication.

A higher assurance is required for dealing with high price goods; on the contrary, such a careful user authentication is not required in case of dealing with low rice goods and it is necessary to confirm securely the request by the subject in case of dealing with those involving a high level privacy such as clinical records.

[0018]

The level of authentication for security may be predetermined for each authentication access terminal or each transaction, or it may be set for every transaction by the authentication access terminal. Alternatively, it may be automatically selected according to the sale price or other appropriate guidelines.

Further, in this process of dividing information, even when whole biological individuality data are used for user authentication, because the authentication is executed at the authentication access terminal deriving most of the data from the user authentication card, the amount of information exchanged through the communication line can be reduced, and hence the traffic flows on the communication line and the time spent on inquiring can be

reduced.

The division of information has also effects on the control of processing performance and memory capacity at the certification authority which is required to store information of a large number of users and to dispose a lot of inquiries.

[0019]

Furthermore, the user authentication system may include a registration authority provided with a memory device for storing biological individuality data of the user obtained at the registration station. The registration authority holds the full records of the biological individuality data of the user obtained at the registration station for use in judging the location where unauthorized use of data or an abnormal condition has occurred, reissuing a damaged authentication card, or repairing the data of the lower certification authorities.

[0020]

At the registration authority, the memory medium recording the biological individuality data may be removed from the information communication channel of the user authentication system so that it can be connected only when it is necessary. This makes it possible to prevent raid by hackers, and hence the leakage and falsification of personal information.

For security, it is extremely effective that only a part of the user's biological individuality data are recorded in the user authentication card and the lower certification authorities, respectively, so that integrity of the data is not allowed to be at one place.

[0021]

The biological individuality data used in the user authentication system of the invention may include handwriting. The handwriting well represents a biological individuality of each person and is effective in preventing others from imitating the individual's, and besides, the input device or analyzer is relatively

easy to find. The user can write arbitrary letters or figures as his or her identification, but it is more desirable that the user writes his or her signature because of its better reproducibility.

The biological individuality data may also include a fingerprint, a voiceprint, an iris or retina pattern, and DNA information. Further, it is probable to find other biological individualities recognizable more easily and securely, in future.

[0022]

The biological individuality data may be divided physically as recorded in the user authentication card and in the certification authority. For example, the first half and the second half of the biological individuality data may be recorded in the authentication card and in the certification authority, respectively, and checked separately. Alternatively, the information may be hierarchically divided such that information on the shape of handwriting is recorded in the user authentication card and information on the stroke pressure and stroke order is recorded in the certification authority.

Further, plural kinds of biological individuality data such as a signature and a voiceprint may be recorded separately to judge the personal identification based on different kinds of information so as to improve the reliability.

[0023]

Furthermore, plural kinds of biological individuality data may be registered and make different transaction conducted in response to the type of input data.

In addition to the normal data of biological individuality, other unique information may be used together which is effective only in a special case. For example, in a case where a user is compelled to put his or her signature under the threat or duress by another person, the user can secretly add a hidden

symbol or sign in his or her signature to notify a security firm of the emergency situation while making the threatener believe that he or she obediently puts his or her signature in usual way.

[0024]

As an option on this scheme, it may make a show of normal transactions such as to unlock a door or to withdraw cash in order to ensure personal safety in such an emergency case.

Such biological individuality data as to use for the emergent purpose may be the same type as that of normal data, or combined data of plural different types such as to add voice data to a signature.

Reversely, combined data with special code data added to dummy data may be used as correct authentication data.

[0025]

A user authentication card used of the present invention is a memory medium provided with a readable memory area which stores a signal for identifying the authentication card and at least part of the biological individuality data for distinguishing the individuality of a user from others to solve the aforementioned objects.

The memory medium may be a read-only memory medium such as a ROM or CD-ROM, but a writable/readable memory medium may be possibly adopted which can add records of transaction details or new information because there is less danger of falsifying the contents of the record indicative of biological individuality data of the user therein.

[0026]

It is desirable to use a high-security IC card having a high counterfeit-proof function and a large data space, mounting an intelligent function and an encryption system thereon.

If an IC card with a CPU and a RAM mounted thereon is used, the IC card can take biological individuality data of the user in the card and compare them with checking data stored inside for authenticating user identification. In this case, the load of the authentication access terminal and the device cost of the terminal can be reduced. Further, the authentication data of the user authentication card can be made unreadable from the outside for improving the security.

[0027]

The use of an IC card enables to provide a multi-purpose card for achieving a high level of personal authentication with multiple functions mounted thereon. The IC card used here may be a composite type provided with a contact type that reads and writes data through an external terminal and a non-contact type that reads and writes data in a non-contact way without the external terminal.

In particular, if the information is dividedly recorded, since it is useless to falsify the contents of the record in the user authentication card of the present invention, an economical and easy-to-use medium such as a floppy disk can be used as the user authentication card. There can be also used other writable media such as a CD-ROM, a DVD, a recording tape, or an MD.

[0028]

In order to solve the aforementioned objects, a user authentication device of the present invention includes an authentication-card reader for reading out information recorded in the user authentication card, an identity acquisition unit for obtaining biological individuality data of a user, a judgment unit for collating the biological individuality data in the authentication IC card read out by the authentication-card reader with the biological individuality data obtained on the spot through the identity acquisition unit and judging the acceptance, and a

display unit for displaying the judgment result.

[0029]

According to the user authentication device of the invention, the user who is requested to authenticate personal identification puts the user authentication card in the authentication-card reader, and inputs through the identity acquisition unit his or her biological individuality data of the same kind as that recorded in the user authentication card. As a result, the judgment unit checks the biological individuality data recorded in the user authentication card with that obtained by the identity acquisition unit and judges whether the checking result is acceptable, while the display unit indicates the judgment result. Thus, the person carrying the user authentication card can be judged immediately to be a proper card holder or not without external communication.

[0030]

The user authentication device should be equipped with the identity acquisition unit of the same type as the biological individuality input device used in the user registration station. A device having a function to take in handwritten figures may be used as the identity acquisition unit. The handwritten figure acquisition unit can input the predetermined handwritten figure, such as a signature, as digital data and easily compare the input figure with the biological individuality data on the user authentication card.

[0031]

The user authentication device of the invention preferably includes a communication unit for communicating with an outside certification authority, in which at least part of the biological individuality data of the user input through the identity acquisition unit is sent to the outside certification authority so that the user authentication device can receive the pass/fail judgment result from the certification authority and display the result through the display unit.

If the user authentication device is connected to the outside certification authority for hierarchical processing of the authentication data, invaders' evil access or falsification can be prevented, and this makes it possible to offer authentication performance with a higher level of security.

[0032]

Detailed Description of the Preferred Embodiments

The present invention will be described in detail based on the embodiment with reference to the drawings.

Fig. 1 is a block diagram illustrating a user authentication system as practiced in an embodiment of the present invention. Fig. 2 is a perspective view illustrating an example of a user authentication device used in the embodiment. Fig. 3 is a diagram of the user authentication device of the embodiment. Fig. 4 is a block diagram illustrating the examples of a user authentication card used in the embodiment. Fig. 5 is a flowchart illustrating the process of issuing the user authentication card in the embodiment. Fig. 6 is a flowchart illustrating the process of authentication at an access terminal in the embodiment.

[0033]

Embodiment 1

As shown in Fig. 1, the user authentication system of the embodiment is of hierarchical structure in which an authorized registration authority, certification authorities, and authentication access terminals are arranged hierarchically.

The authorized registration authority or the policy registration authority (PRA) 1 supervises the entire authentication network and issues certificates of commission of partial power to a plurality of intermediate certification authorities or policy certification authorities (PCA) 2 as licensees. The policy certification

authorities given the power then issues certificates of commission of partial power to a plurality of end certification authorities (CA) 3 as sub-licensees.

[0034]

The end certification authorities (CA) 3 act as go-betweens in connecting authentication access terminals (TM) 4 as clients who make use of user authentication, and users 8 who enjoy services offered by the clients. In the following description, access to various services may be called "transaction."

The authorized or policy registration authority (PRA) 1 is provided with a memory 11 removable from the main equipment, while the policy certification authorities (PCA) 2 and the end certification authorities (CA) 3 are provided with memories 21, 31 connected to respective equipments at all times.

[0035]

These facilities are connected with each other through dedicated lines or public lines, so that information can be exchanged at any time. The connections may be made via the intranet or the internet. In exchanging information through the communication lines, it is preferable to ensure security through an encryption system using public keys or common or symmetric keys.

The policy certification authorities (PCA) can be eliminated from the user authentication system. The policy certification authorities (PCA) can be provided over plural levels to increase the depths of the hierarchy to more than three.

The policy registration authority (PRA), the policy certification authority (PCA), and the end certification authority (CA) may also be replaced by an institution which integrates all the functions.

[0036]

The end certification authorities (CA) are generally empowered by the policy registration authority (PRA) or an upper certification authority (PCA) to

execute authentication in a limited region such as a public administrative agency, a medical institution, a specific company, an apartment building, a mall, and the like.

The end certification authority (CA) 3 is connected to authentication access terminals (TM) 4 which belong to the limited region and use the authentication.

[0037]

The authentication access terminals (TM) 4 may represent a window of a government office, a division reception desk or pharmacy reception desk in a hospital, a door in a laboratory or office, an information tool accessing a database to be protected, an apartment entrance or an apartment door, a remote control device for indoor utilities, a member-only club facility, a checkout counter at each store in a mall or in a large retail store such as a department store, a window in a monetary facility such as a bank, an automatic teller machine, and so on.

In particular, it is considered that user authentication will be more important in the field of direct marketing hereafter. In this case, the authentication access terminal 4 may be placed in home of each user 8.

[0038]

The end certification authority (CA) 3 authorizes a user registering station (RG) 5 to receive a registration application from a user 8 who wants to be a consumer of an authentication access terminal (TM) 4, and authorizes an authentication-card issuing station (IS) 6 to issue user authentication cards 7.

[0039]

The user registering station (RG) 5 is furnished with an input device 51 for obtaining biological individuality data. This embodiment uses an on-line handwritten-figure input device with a tablet and a pen. The on-line

handwritten-figure input device input handwriting of a user with the process of writing for graphic recognition, so that, when letters are input, the information on direction and order of each stroke of letters can easily be obtained.

[0040]

When a voiceprint is used as means of capturing the biological individuality, a microphone 52 is equipped for input user's voice. Any other device, such as a fingerprint or palm-print input device, or a device for observing a pupil to take in an iris or retina pattern, can also be provided.

The use of a plurality of personal identification means makes the authentication more securely.

[0041]

The authentication-card issuing station (IS) 6 is furnished with an authentication-card issuing device 61. The authentication-card issuing device 61 writes the information to be used for user identification in a user authentication card 7 and issues the authentication card to the user 8. In this embodiment, the user authentication system uses an IC card as the user authentication card. However, any other recording medium can be used as long as it is available for write and read operations, i.e., any other electronic recording medium can be used, such as a magnetic recording medium including a CD-ROM, a floppy disk, and a magnetic card, or a magneto-optic recording medium.

[0042]

The authentication access terminal (TM) 4 is furnished with a user authentication device 41 that examines genuineness of the user authentication card 7 carried by the user 8 and authenticate the user 8.

Figs. 2 and 3 show an example of a configuration of the user authentication device 41.

Arranged on the front panel of the user authentication device 41 are an input/output unit 401 with a slot for inserting an authentication card 7, which exchanges information with a memory area of the inserted authentication card 7; an authentication-level specifying unit 402 that specifies the depth of authentication required for the current transaction; a personal identity input unit 403 that takes in a biological individuality data of the user; and an authentication display 404 that displays the authentication result.

[0043]

The personal identity input unit 403 is the same as the biological individuality input device 51 used at the user registering station (RG) 5. If the voiceprint is used together in user authentication, a microphone 42, of course, needs to be provided to the user authentication device 41 of the authentication access terminal (TM) 4. The personal identity input unit 403 is thus equipped with respective input means corresponding to types of the biological individualities to be used.

[0044]

Electronic circuitry 410 is incorporated inside the user authentication device 41; it acts to organically combine the functions of these units for user authentication.

The electronic circuitry 410 includes an authentication card read/write control part 411, an identity information converting part 412, a judgment part 413, and a communication part 414.

The authentication card read/write control part 411 has the functions to read the contents of information recorded in the authentication card through the input/output unit 401, to decode the encrypted digital data, and to record the transaction results onto the authentication card as well.

[0045]

The identity information converting part 412 converts the biological individuality data taken in by the personal identity input unit 403 to digital data.

The judgment part 413 takes in output information from the authentication card read/write control part 411, the identity information converting part 412 and the authentication-level specifying unit 402, authenticates user identification according to the level of required authentication based on those output information added with information exchanged with the certification authorities through the communication part 414, and indicates the authentication result through the authentication display 404.

[0046]

When the user is authenticated and a transaction is established, then the transaction result is input from a transaction-detail input unit 420 and the transaction details are displayed on a transaction display 421, so that the user 8 can confirm the transaction details. The transaction details are also recorded in a memory 422.

The judgment part 413 may be designed to automatically send the user authentication result to the transaction-detail input unit 420 so that the transaction may be determined to be accepted or refused.

[0047]

Further, the transaction details or transaction history may be recorded in the user authentication card 7 by inputting the transaction information via the transaction-detail input unit 420.

As an example, when the user authentication card 7 is used for settlement purpose, the purchasing date, purchased product names, and their prices can be recorded, and those make it easy for the user to confirm the transaction at payment. When the card used for administrative services, information related to various certificates or identification papers such as health

insurance card, driver's license, medical record and certificate of residence, can be received and stored in the user authentication card 7.

Privacy of the user can be protected by requiring user authentication anytime when a person reads the contents recorded in the user authentication card 7 so that any access by all but the user concerned shall be prohibited.

[0048]

In addition to the biological individuality data used for normal authentication, other unique information that is effective only in special cases may be used together. For example, in a case where a user is compelled to put his or her signature under the threat of a robber or duressor, the user can secretly add a hidden symbol or sign in his or her authentic signature to notify a security firm of the emergency situation while normal transactions are taking place such as opening a door or withdrawing cash, so that the security officers can take appropriate action such as to arrest the criminal as soon as the safety of the user is ensured.

Such biological individuality data as to use for special purposes may be combined data of plural different types such as twice coughs at the time of signature.

[0049]

Fig. 4 is a block diagram illustrating internal arrangements of the user authentication card 7 made of an IC card.

The user authentication card 7 as practiced in the embodiment is a composite-type IC card provided with a contact type connector transmitting electric signals through a terminal 71 and a non-contact type connector establishing communication by means of electrostatic coupling or electromagnetic induction without contact between an electrode 73 in the card and an electrode inside the authentication card read/write control unit. The user

authentication card 7 is designed in consideration of a case where plural card issuers place a commonly usable terminal, respectively, for a single common card to be openly used by its carrier for respective issuers. The IC card, however, may be provided with either one of the connectors.

[0050]

The terminal 71 is connected to a connection circuit 72; the non-contact type electrode 73 is connected to a communication control circuit 74. Both are coupled with built-in memories.

The user authentication card 7 also includes a CPU 75 and memories comprising of a random access memory RAM 76, a read-only memory ROM 77, an electrically-writable, programmable read-only memory PROM 78, and an electrically-erasable, programmable read-only memory EEPROM 79. These are connected with each other through a bus.

The connection circuit 72, the communication control circuit 74, the CPU 75 and the memories can be mounted on a single IC chip.

[0051]

Upon insertion of the user authentication card 7, the authentication card read/write control unit 411 accesses the memories of the user authentication card 7 either from the terminal 71 through the connection circuit 72, or from the non-contact electrode 73 through the communication control circuit 74.

The PROM 78 stores card authentication data for examining the authenticity of the authentication card concerned and an ID of issuer that has issued the user authentication card upon approval, and the like. The data once written in the PROM 78 cannot be renewed.

The EEPROM 79 stores biological individuality data for use in authenticating user identification and the record of transactions executed using the authentication card. The ROM 77 stores programs for control of the CPU

75 to execute encryption and decryption, control of data input/output, examination of the authenticity of the user authentication device 41, and so on. The RAM 76 temporarily stores data taken from the outside and data needed in the computing process, and so on.

[0052]

Unused user authentication cards 7 are distributed to each authentication-card issuing station 6 on the condition that correct card certificate information has been written in the PROM 78 at the authorized or policy registration authority 1 to prove that the authentication cards are genuine cards available in the system. Therefore, all the authentication-card issuing station 6 has to do is to write in part of biological individuality data of the user in the EEPROM 79 in accordance with instructions by the authorized registration authority 1. In this regard, the writing function of the PROM 78 may be omitted from the authentication-card issuing device to prevent the card from being falsified.

The authentication card is not limited to the arrangement or allotment of the memories as practiced in the embodiment. For example, the biological individuality data for use in authenticating personal identification may be stored in the PROM 78 or RAM 76.

[0053]

The following section describes, along with Fig. 5, an example of the process of issuing a user authentication card.

The user registering station 5 accepts a registration application from a user 8 who wants to receive services at authentication access terminals within the territory of the user registering station 5 (S11). The user registering station 5 gathers information indicative of biological individualities of the user, and if necessary, information for use in pre-qualifying the user 8 (S12). The

biological individuality data used here are characters unique to the user's living body; they should be selected for characteristics through which the user can be distinguished from others in disguise or in imitation of the user.

[0054]

In the embodiment, handwriting is used for identifying the user. Although any figure is possible, if the user 8 inputs different figures every time, it would be inconvenient to authenticate personal identification. It is therefore desirable for the user to put his or her own signature so as to secure the reproducibility. In addition to the handwriting, the use of plural biological individuality data can improve the security of authentication, and hence, the auxiliary microphone 42 is provided here for acquiring voiceprints.

The qualification information and the biological individuality data of the applicant, both gathered at the user registering station 5, are then transmitted to the authorized registration authority 1 (S13).

[0055]

The authorized registration authority 1 pre-qualifies the applicant based on the information from the user registering station 5, and permits the issue of an authentication card to the applicant who has passed in the pre-qualification (S14). The qualified conditions depend on the target services for which the user requests the authentication. In this regard, the end certification authority 3 that actually accepts the user may examine the qualification of the user.

The authorized registration authority 1 divides the biological individuality data of the registered user 8 hierarchically into data parts according to predetermined proportions, decides the parts to be assigned to the user authentication card 7 and the certification authorities 2, 3, respectively, and distributes them to each place (S15).

[0056]

The biological individuality data distributed from the authorized registration authority 1 to each place is to be accessed based on the authentication accuracy required by the authentication access terminal 4. If the authentication access terminal 4 requires the least-level of authenticity, the authentication needs only the checking result of the authentication device 41 of the authentication access terminal 4. If a medium-level of authenticity is required, the user is to be authenticated based on the checking result of the authentication device 41 plus the information stored at the end certification authority 3. If the highest-level of authenticity is required, all the biological individuality data distributed to all the different places should be integrated for the judgment.

[0057]

The user authentication system of the invention is constituted such that further authentication by the upper authorities based on the biological individuality data can be requested only when the authenticity has examined and passed at the authentication access terminal. The upper authorities execute authentication based on the information except included inside the user authentication card.

Therefore, the user authentication card 7 needs to be distributed with information enough for certification with a degree of accuracy by comparing with biological individuality data input by the user at the spot so that the user can be judged to be authentic.

[0058]

In this embodiment, 60 % of information is assigned to the user authentication card 7, 30 % to the end certification authority 3, and the rest of 10 % to the intermediate authority 2. Such a gradual decrease of information amount can not only save the memory capacities at the upper authorities, but

reduce load time for each authentication as well, thereby improving information protecting performance throughout the entire system.

[0059]

It should be noted that it is desirable for the user authentication card 7 to hold a relatively high percentage of biological individuality data so as to prevent excess amount of information from being transmitted to the upper authorities upon request to execute a higher-level of authentication.

On the contrary, excess percentage of information to be assigned to the user authentication card 7 may lower the reliability of user authentication.

It is therefore essential to distribute the biological individuality data in dividing proportions adapted to each practical conditions in consideration of number of user accesses, required level of authentication security, and so forth.

[0060]

Information may be divided such that all the digitized data is divided physically in predetermined proportions, or divided on the step-by-step basis. For example, information of handwriting may be divided into information related to a final figure of handwriting, information related to stroke on the way of writing, and information on the stroke order. Any biological individuality data can be divided for use in each related spot, for example, a voiceprint can be divided by frequency band, or a fingerprint can be divided by finger.

In the case a plural types of biological individuality data such as handwriting and a voiceprint are extracted, the biological individuality data may be distributed by type.

[0061]

The authorized registration authority 1 stores information related to the authentication card and the user in a large-capacity memory means 11 removable from the main device, such as a magnetic tape, a CD-ROM, a

magneto-optical disk, a DVD, or a removable hard disk (S16), and upon receipt of a request from a lower authority, a person in charge inserts the memory means into a driver in order to check the registered information.

At the authorized registration authority 1, the removable recording medium 11 is stored by separating it from an external communication network when it is not in use so as to prevent violence or falsification of records.

[0062]

The certification authorities 2, 3 stores distributed part of the biological individuality data of individuals into the memories 21, 31, respectively, and reads out it on demand.

The authentication-card issuing station 6 records the part of biological individuality data of the registered applicant distributed by the authorized registration authority 1 in a user authentication card 7 which records its own card authentication code, and issues the card 7 to the user 8 (S17).

[0063]

A plurality of user registering stations (RG) 5 and authentication-card issuing stations (IS) 6 can belong to a single end certification authorities (CA) 3.

Further, since the user 8 is required to go to the user registering station 5 and input his or her biological individuality data, the authentication-card issuing station 6 for issuing the card to the user 8 is convenient for the users if it locates at the same location as the user registering station 5.

[0064]

It may also be useful to have a reliable witness to identify the user 8. But it is hard for any mechanism to exclude a person pretending to be another person from the beginning.

Further, the authentication card is not necessarily issued immediately after the registration procedures, and it may be mailed later to the user's

address in order to confirm the facts the user has declared.

Furthermore, the user registering station (RG) 5 and the authentication-card issuing station (IS) 6 may belong to the authorized registration authority (PRA) 1.

Furthermore, an issuer can conduct registration/issue procedures at any place if the issuer carries a portable terminal having the same functions as those provided at the user registering station (RG) 5 and the authentication-card issuing station (IS) 6. The use of such a portable terminal should be restricted to only the issuers who have been authentically licensed by the authorized registration authority (PRA). Even in this case, the issuer is never permitted to use the portable terminal without passing in strict examination and receiving a certificate of issuer.

[0065]

The following section describes, along with Fig. 6, an example of the process of authenticating user identification using a user authentication card 7 at an authentication access terminal 4.

When a user 8 presents his or her user authentication card 7 and applies to a transaction at an authentication access terminal 4, the user authentication card 7 is inserted into the card slot (input/output unit) 401 of the authentication device 41 of the authentication access terminal 4 to read out the authentication information from the user authentication card 7. The authentication information includes information for confirming the authenticity of the card and biological individuality data for use in authenticating user identification.

[0066]

At the authentication access terminal 4, the card is authenticated first (S21). The card authentication confirms that the user authentication card 7 is authentic, i.e., that the card is adapted to the user authentication system for use

at the authentication access terminal 4, and that the person is the authentic holder of the card. If the user authentication card 7 is not adapted to the authentication system, any transaction will not be accepted at the authentication access terminal 4 from the very first.

It should be noted that, in order to confirm that the user authentication card 7 is not accessed by an unauthorized device, there may be provided a mechanism in which a program in the user authentication card 7 verifies whether the authentication device 41 is qualified to the authentication card itself, and if the device is not proper, the authentication card rejects the disclosure of the stored contents.

[0067]

When the user authentication card 7 has passed in the authentication, the user 8 is then required to show the same biological individuality as the user deposited when obtaining the user authentication card 7, e.g., to put his or her signature on the tablet (personal identity input unit) 403 (S22).

The biological individuality data input from the tablet 403 is checked against the biological individuality data recorded in the user authentication card 7, which is, for example, 60 % of the biological individuality data of the user, and the user 8 at the window is judged to be the authentic holder of the user authentication card 7 or not (S23). The user authentication result is displayed on the display 404 (S24).

[0068]

The subsequent procedures at the authentication access terminal 4 vary according to whether the user has been authenticated or not (S25). If the user authentication is negative, the authentication access terminal 4 will reject any transaction (S33). If the user authentication is affirmative, it is checked whether or not further on-line authentication is to be requested from upper

authentication institutions (S26). If no on-line authentication is needed, the authentication access terminal 4 may accept the transaction applied by the user 8 at once (S32).

The presence or absence of request and the depth of the request for the on-line authentication may be input by an operator or the user 8 with the authentication-level specifying unit 402 at every transaction, or may be automatically set based on nature of the transaction or the transaction money.

[0069]

If the on-line authentication is needed, a request for a certain level of authentication is sent to the end certification authority 3, together with the information of the user authentication card 7 and the personal identity information obtained at the personal identity input unit 403 (S27). The personal identity information to be sent can be a part, for example, 40 % of the personal identity information, exclusive of the part used at the authentication access terminal 4, so that the quantity of information exchanged between the authentication access terminal 4 and the end certification authority 3 can be reduced.

[0070]

The necessity of the on-line authentication should be determined according to the level of security required based on the nature of the transaction. Specifically, commercial transactions about highly realizable goods or expensive goods, disclosure of personal information, and something like that require secure authentication; such transactions should request user authentication of upper authorities.

The depth of on-line authentication may also be specified by the nature of the authentication access terminal 4. For example, at a hospital reception desk, a high level of authentication of personal identification may often be

required to protect a person's privacy and insure accurate medical treatment. Especially, in case of telecommuting medical treatment, it is preferable to request user authentication from the upper authorities.

[0071]

The information sent to the end certification authority 3 is checked with the identity information characteristic of the user 8, the identity information stored in the memory 31 (S28), and the authentication results are forwarded to the authentication access terminal 4 (S29).

Since the end certification authority 3 has only the record for 30 % of the identity information on the user, if the user authentication at the end certification authority 3 is insufficient, further user authentication will be requested from the policy certification authority 2. Since the policy certification authority 2 has only the record for 10 % of the identity information on each user, the policy certification authority 3 uses 10 % of the identity information obtained at the authentication access terminal 4, so that the information to be sent from the end certification authority 3 to the policy certification authority 2 can be vastly reduced.

The user authentication results of the policy certification authority 2 are sent back to the authentication access terminal 4 through the end certification authority 3.

[0072]

The user authentication results of all the authenticating facilities are integrated into a resultant total output and displayed on the authentication display 404. If the total result satisfies the user authentication, the transaction is accepted (S32), and if not satisfy, the transaction is rejected (S33).

When the user authentication is denied, there is a possibility of any fraud such as the falsification of records or disguise of the user. In this case, it is

preferable to send the information to the authorized registration authority 1 and to analyze the troublesome and its cause.

[0073]

Since the authorized registration authority 1 stores protected records that is difficult to invade or falsify from the outside, the records of the authorized registration authority can be compared with the data input at the authentication access terminal 4 to make it clear where the abnormal conditions occurred among the user authentication card 7, the end certification authority 3, and the policy certification authority 2.

If the contents of the user authentication card 7 do not match with the information input by the user 8, it should be considered that the user authentication card 7 got into wrong hands, such as a case where another person who is not the authentic user picked up or robbed the user authentication card 7, or where the data of the user authentication card was rewritten by unauthorized access.

[0074]

Embodiment 2

The user authentication system as practiced in the second embodiment differs from the first embodiment only in that the user authentication card has an operation function to check the biological individuality data of the user with the identity information recorded thereon, in stead of the use of the logical arithmetic unit provided at the authentication access terminal to check the biological individuality data input from the personal identity input unit with the biological individuality data recorded in the user authentication card. Referring here to the same drawings as used for describing the first embodiment, only the different portions from the first embodiment are described.

[0075]

On an IC card used here as the user authentication card 7, certain elements such as the CPU 75 and RAM 76 can be mounted to have a certain operation function.

In the system of the embodiment, a user 8 who wants to receive services at an authentication access terminal 4 inputs his or her own biological individuality data through the user authentication device 41. The biological individuality data are then processed accordingly, converted into digitized form, and sent to the user authentication card 7.

[0076]

The user authentication card 7 stores the input information data into the RAM 76 temporarily. The CPU 75 then reads out the biological information data of the authorized user from the EEPROM 79, and compares the information data temporarily stored in the RAM 76 with the information data read out from the EEPROM 79. If the comparison shows that all the points of similarity between either information data are within an acceptable range, the person asking for services at the authentication access terminal 4 is authenticated as the true holder of the user authentication card 7, and the authentication access terminal 4 is notified of the acceptance. If the person has not passed in the authentication, the authentication access terminal 4 is notified of the refusal.

[0077]

After accepting the user authentication result from the user authentication card 7, the authentication access terminal 4 offers desired services to the user 8. If more careful authentication is needed, the authentication access terminal 4 inquires the end certification authority 3 or the policy certification authority 2 to further authenticate the person in accordance with the authentication results from the upper authorities. It should be noted that the authentication access

terminal 4 may be combined with the end certification authority 3.

Although the proportions of biological information data distribution among related spots can be determined arbitrarily, it is advantageous to allocate a higher percentage of biological information data for lower-level authentication as shown in the first embodiment. This makes it possible to reduce a communication load of the entire system, and hence to improve the system operability. It is therefore preferable to allocate the user authentication card 7 more than 60 % of the biological information data.

[0078]

In the embodiment, the system makes use of an intelligent IC card as the user authentication card 7 not only to reduce the calculation load of the user authentication device 41, but to decrease the device cost as well. Therefore, the smaller cost for preparing the facilities at the authentication access terminal 4 lowers barriers for clients to join the system, thereby enhancing the availability.

Further, since all the information processing is completed inside the user authentication card, the authentication card can be provided with a readout prohibited area for recording important information as authentication data which prohibits any outside parties from access. This makes it possible to prevent secret information from leaking, and hence to improve security.

[0079]

Effects of the Invention

As described in detail hereinabove, if the user authentication system of the present invention is used, a user authentication corresponding to the required level of security can be obtained, by performing the majority of information processing at the authentication access terminal without charging a large load to the communication channel, because the identity information input directly by the user at the authentication access terminal and the biological

individuality data in the authentication card are compared, and a part of the identity information is transmitted to an authentication authority of the higher order for further authentication in case where a higher level of assurance is desired.

Brief Description of Drawings

Fig. 1 is a block diagram illustrating a user authentication system as practiced in an embodiment of the present invention;

Fig. 2 is a perspective view illustrating an example of a user authentication device used in the embodiment;

Fig. 3 is a circuit diagram of the user authentication device of the embodiment;

Fig. 4 is a block diagram illustrating the examples of configurations of a user authentication card used in the embodiment;

Fig. 5 is a flowchart illustrating the process of issuing the user authentication card in the embodiment; and

Fig. 6 is a flowchart illustrating the process of authentication at an access terminal in the embodiment.

Explanations of numerals

1	Policy registration authority
11	Removable memory
2	Policy certification authority
21	Memory device
3	End certification authority
31	Memory device
4	Authentication access terminal
41	User authentication device
5	User registering station

51 Personal identity input unit

52 Microphone

6 Authentication-card issuing station

61 Authentication-card issuing device

7 User authentication card

71 Terminal

73 Non-contact electrode

8 User

ABSTRACT

Problem to be Solved

A user authentication system of higher security allowing to obtain results rapidly, and a user authentication card and a user authentication device used for the same shall be provided.

Means to Solve the Problem

Biological individuality data such as handwriting, voiceprint or the like for distinguishing individuality of a user 8, a user authentication card 7 recorded with at least a part of the biological individuality data thereof, the recorded contents in the user authentication card 7 read out by an authentication card reader 41 are compared with the biological individuality data of the user input to the identity acquisition device for authorizing the used directly at an authentication access terminal. Besides, certification authorities 2, 3 of higher order are provided, and remaining part is recoded in respective certification authorities, without recording all of the biological individuality data of the used in the user authentication card, and the reliability of authentication can be improved by the additional authentication through the comparison of the parts of the recorded biological individuality data in response to an inquiry from the authentication access terminal 4.

Selected drawing: Fig. 1

FIG.1

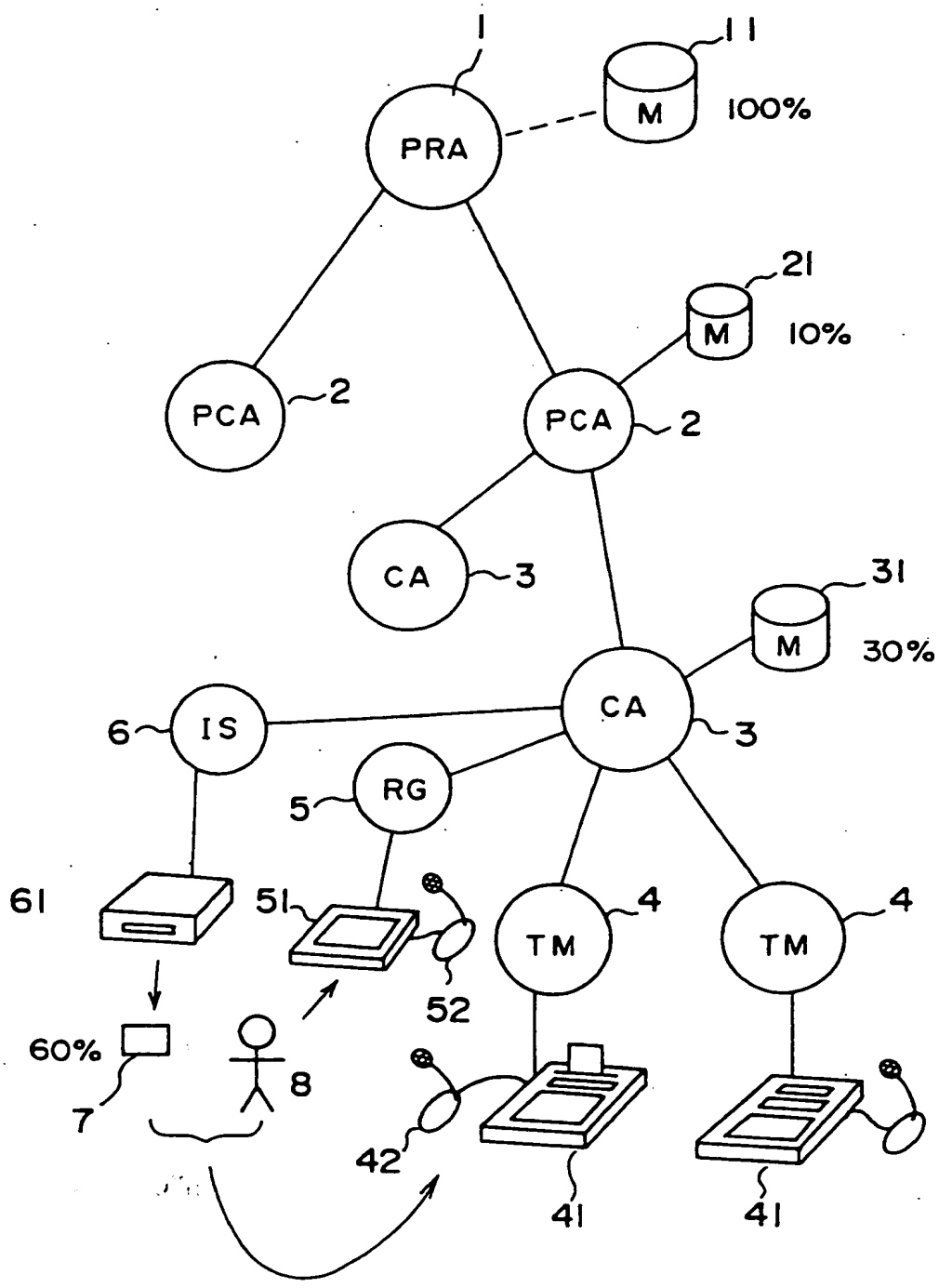


FIG.2

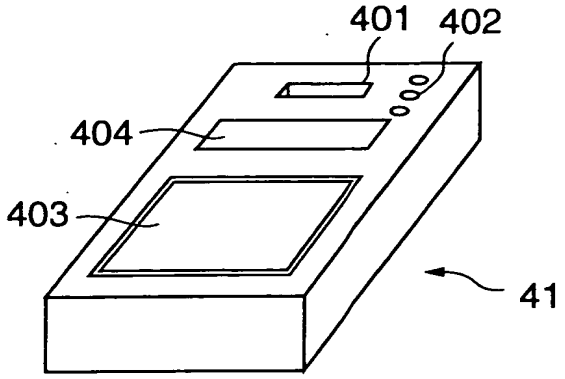


FIG.3

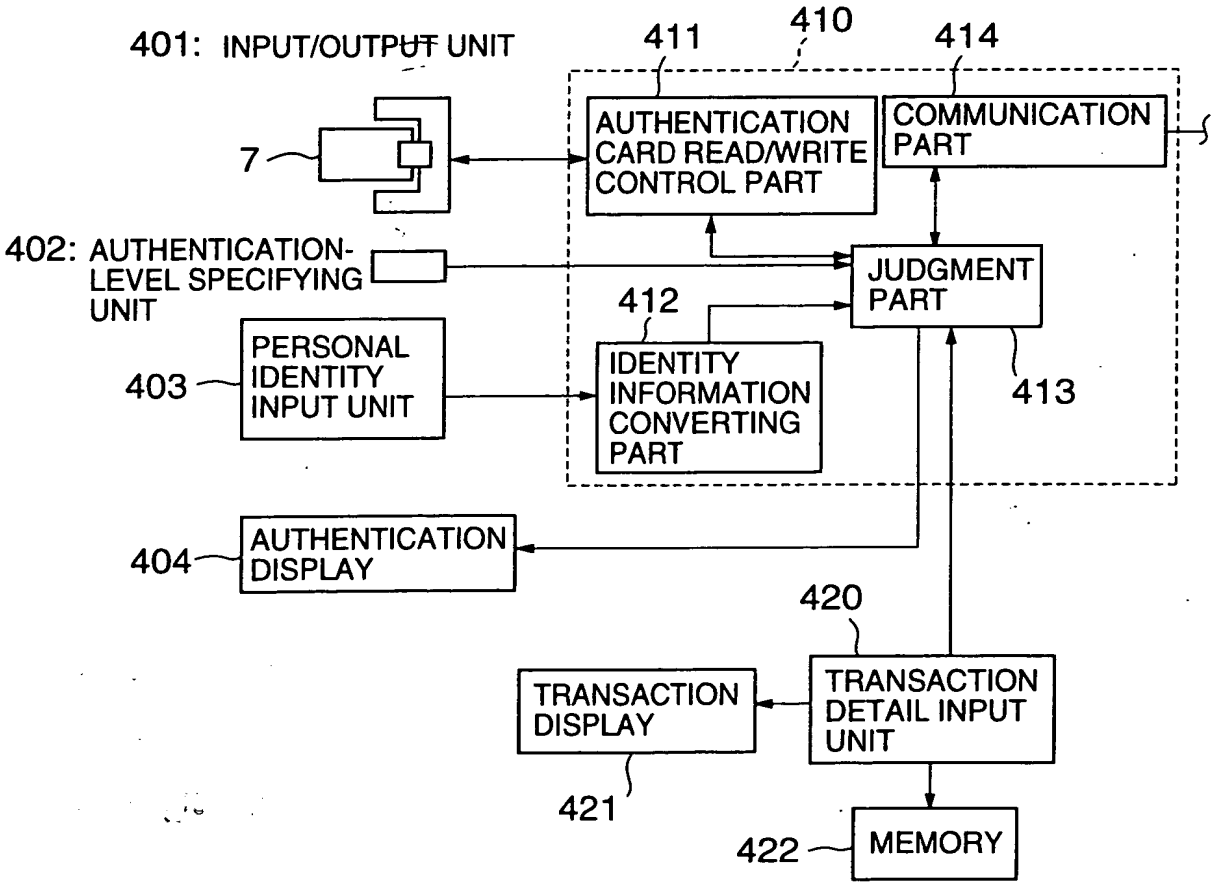


FIG.4

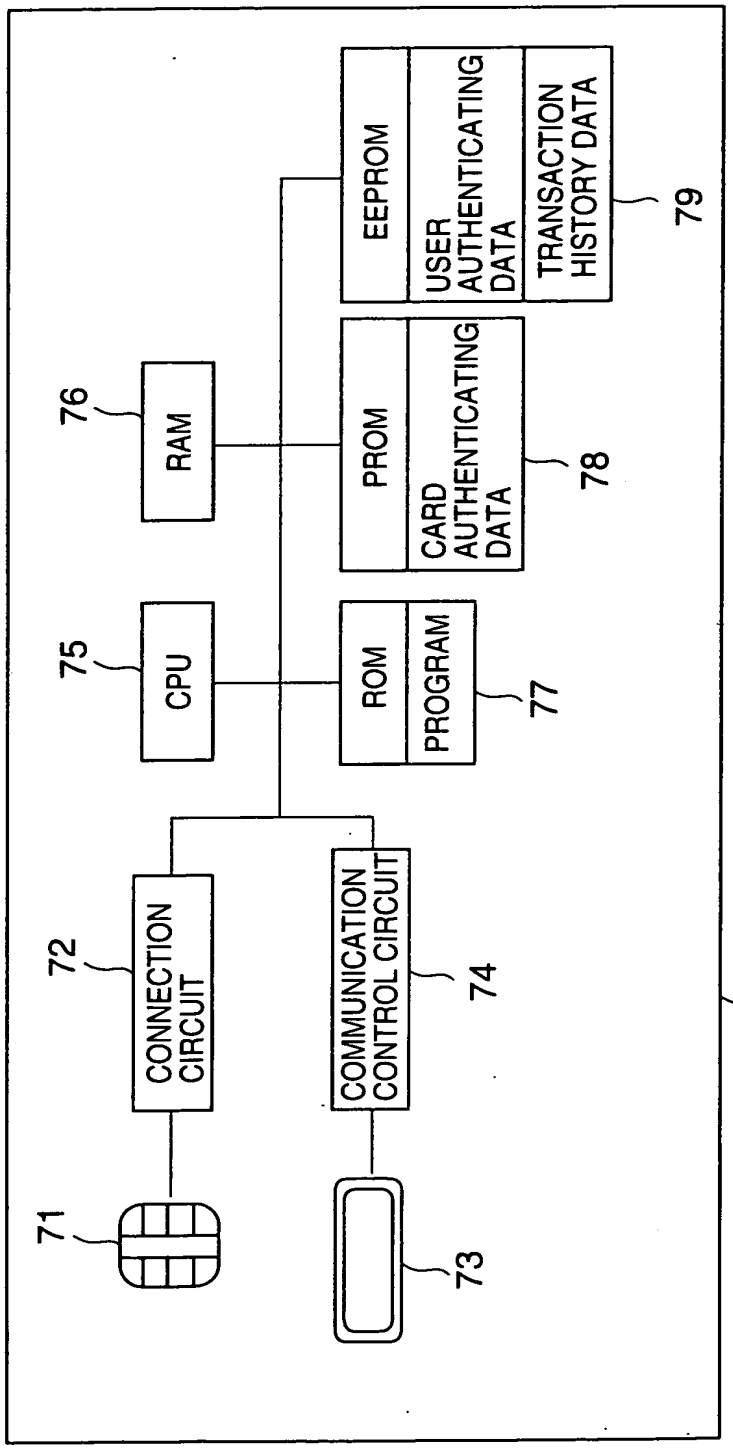


FIG.5

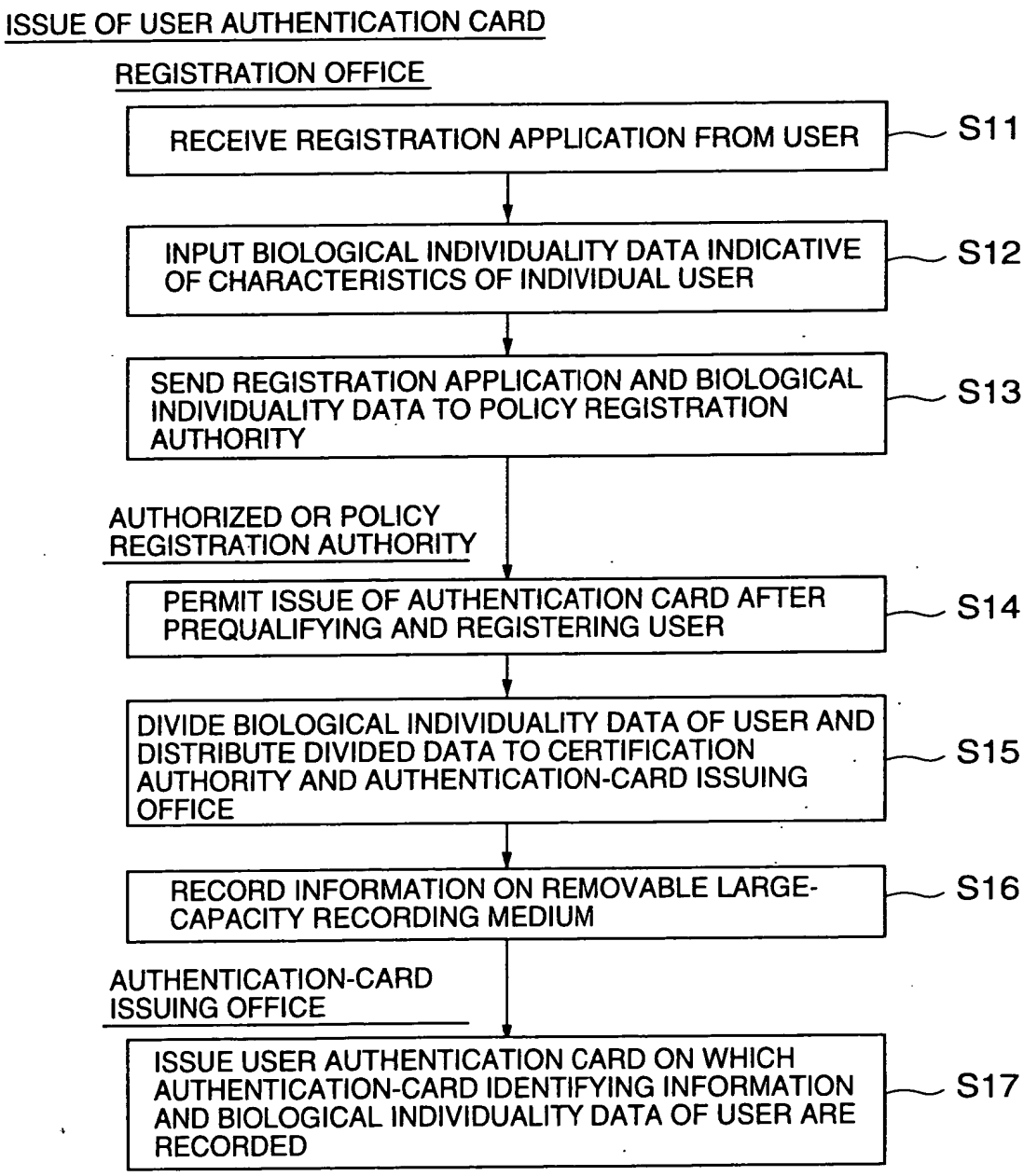
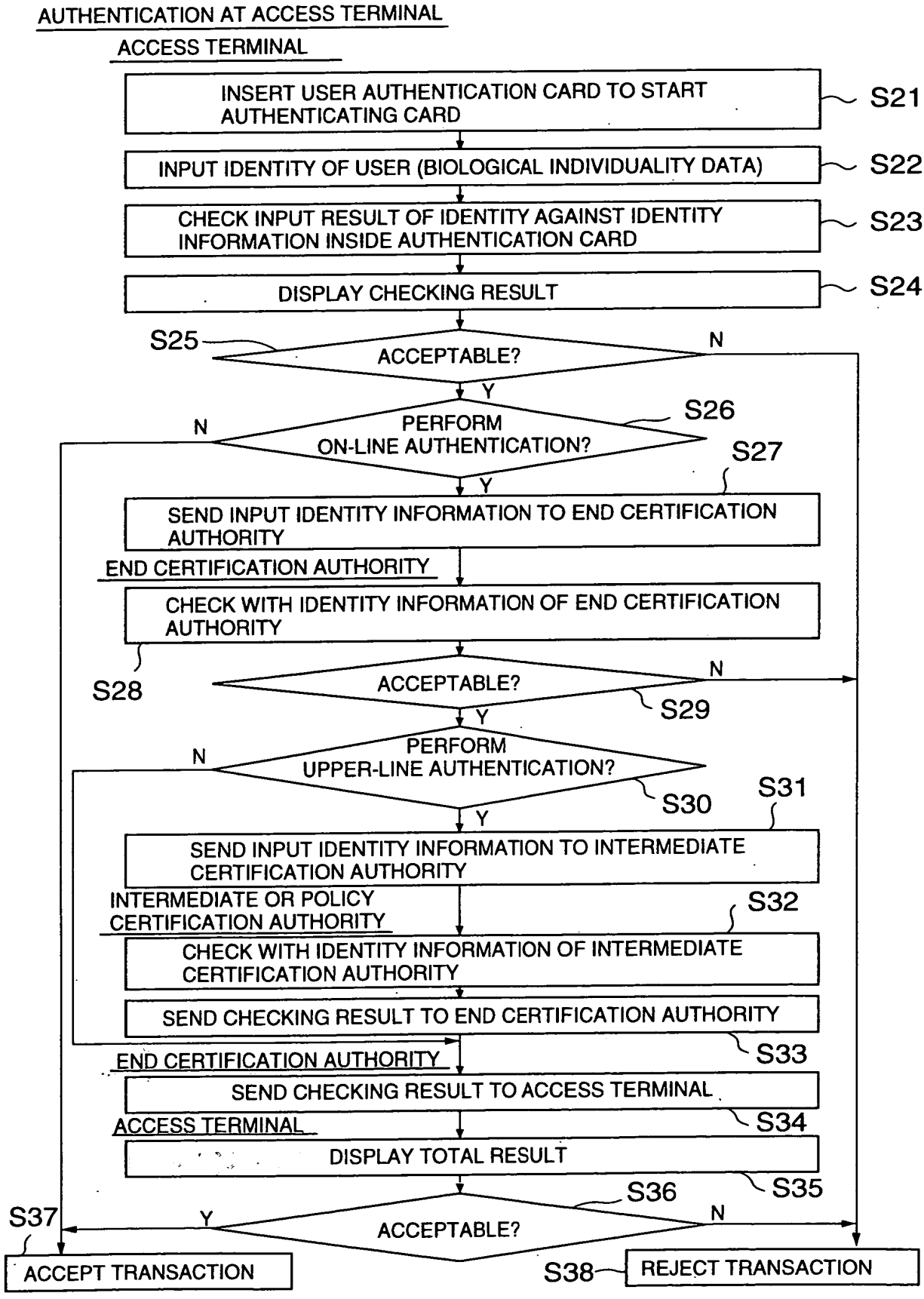


FIG.6



PCT/JP99/02599

日 本 国 特 許 庁

EAKU

PATENT OFFICE
JAPANESE GOVERNMENT

19.05.99

JP99/2599

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９８年　５月２１日

出願番号
Application Number: 平成１０年特許願第１３９５６３号

出願人
Applicant (s): 保倉　豊

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

１９９９年　６月１７日

特許庁長官
Commissioner,
Patent Office

伊佐山建志

出証番号　出証特平１１－３０４１１１３

【書類名】　特許願

【整理番号】　GFS0001

【あて先】　特許庁長官　荒井　寿光　殿

【国際特許分類】　H04L　9/32

G06K 19/00

【発明の名称】　ユーザ認証システムとユーザ認証票およびユーザ認証装置

【請求項の数】　16

【発明者】

【住所又は居所】　千葉県八千代市勝田台南２丁目１５番２２号

【氏名】　保倉　豊

【特許出願人】

【郵便番号】　276

【住所又は居所】　千葉県八千代市勝田台南２丁目１５番２２号

【氏名又は名称】　保倉　豊

【代理人】

【識別番号】　100104341

【弁理士】

【氏名又は名称】　関　正治

【電話番号】　03-3234-4241

【手数料の表示】

【予納台帳番号】　041232

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ユーザ認証システムとユーザ認証票およびユーザ認証装置

【特許請求の範囲】

【請求項１】　ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、該ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを入力する人証取得装置を設けた認証利用所を備えてなるユーザ認証システムであって、該認証利用所において前記認証票読取り装置で読みとるユーザ認証票の記録内容と前記人証取得装置に入力された前記ユーザの生物学的特徴データを比較することにより該ユーザが該ユーザ認証票の正当な所有者であることを認証することを特徴とするユーザ認証システム。

【請求項２】　ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザの生物学的特徴データを取得する人証取得装置と該取得した生物学的特徴データを前記ユーザ認証票に入力する人証情報書込み装置とを設けた認証利用所を備えてなるユーザ認証システムであって、前記ユーザ認証票に記録された生物学的特徴データの内容と前記人証取得装置で取得された前記ユーザの生物学的特徴データを前記ユーザ認証票の演算機能を用いて比較することにより該ユーザが該ユーザ認証票の正当な所有者であることを認証することを特徴とするユーザ認証システム。

【請求項３】　前記ユーザ認証システムがさらに前記認証利用所と情報通信路で接続された少なくとも１個の認証局を備え、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を該認証局に記録しておいて、前記認証利用所からの照会に応えて前記ユーザ認証票において不足する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求項１または２記載のユーザ認証システム。

【請求項４】　前記情報通信路に流す情報は暗号化することを特徴とする請求項３記載のユーザ認証システム。

【請求項５】　前記２個以上の認証局が、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に前記認証利用所もしくは他の認証局からの照会に応えて自己の記憶する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求項３または４記載のユーザ認証システム。

【請求項６】　前記ユーザ認証システムが前記登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えることを特徴とする請求項１ないし５のいずれかに記載のユーザ認証システム。

【請求項７】　前記認証局における生物学的特徴データを記録した記憶媒体が該ユーザ認証システムの情報通信路から切り離せることを特徴とする請求項６記載のユーザ認証システム。

【請求項８】　前記生物学的特徴データが筆跡であることを特徴とする請求項１から７のいずれかに記載のユーザ認証システム。

【請求項９】　前記生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うことを特徴とする請求項１から８のいずれかに記載のユーザ認証システム。

【請求項１０】　請求項１から９のいずれかに記載のユーザ認証システムに用いることのできるユーザ認証票であって、認識票を識別する信号とユーザの個体を区別する生物学的特徴データの少なくとも一部を記録した読出し可能な記憶領域を備えた記憶媒体からなるユーザ認証票。

【請求項１１】　さらにＣＰＵとＲＡＭを備えることを特徴とする請求項１０記載のユーザ認証票。

【請求項１２】　前記記憶媒体が磁気記録媒体であることを特徴とする請求項１０または１１記載のユーザ認証票。

【請求項１３】　前記記憶媒体がＩＣカードであることを特徴とする請求項１０または１１記載のユーザ認証票。

【請求項１４】　ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを入力する人証取得装置と、前記認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと前記人

証取得装置に入力された前記ユーザの生物学的特徴データを比較して合否を判定する判定装置と、判定結果を出力する表示装置を備えるユーザ認証装置。

【請求項１５】　前記人証取得装置が手書き図形取り込み機能を有するものであることを特徴とする請求項１４記載のユーザ認証装置。

【請求項１６】　さらに、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し合否の判定結果を受け取る通信装置を備え、前記表示装置を介して判定結果を表示することを特徴とする請求項１５または１６記載のユーザ認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子情報交換や電子商取引における個人認証を行うためのユーザ認証システムと、これに用いるユーザ認証票、およびユーザ認証装置に関する。

【０００２】

【従来の技術】

近年、通信網を介してアクセスする情報の種類は極めて多様になりつつあり、商品の売買やクレジットなどの電子商取引は勿論、医療におけるオンライン診断や個人カルテ、役所における登録事項の閲覧、証明の発行など、対象もますます増加し、利用が進む傾向にある。

【０００３】

こうした個人的な情報にはプライバシーに係わり他人に漏洩しないという保証がない場合には利用を認めるべきでないとされるものが少なくない。電子情報通信網の発達を取り込んでより便利な情報社会を構築するために、個々人を峻別できる信頼性の高いユーザ認証方式が求められている。

また、個人を正しく認証する機構は、研究所や事業所あるいは住宅などにおける資格者以外の立ち入りを制限する施錠装置などや、電子マネーのセキュリティ向上にも利用することができる。

【０００４】

従来、ユーザ認証にはパスワードが最もよく用いられてきた。パスワードは簡

便であるが、他人のパスワードを盗用して本人に成りすます者を排除することができない。このため、長いパスワードを使う、推測しにくいパスワードを選ぶ、パスワードを時々変更するなど、相応の注意をして安全性を確保しようとする。また、通信過程における安全性を確保するためには暗号化技術を用いて通信内容を秘密化して、データの漏洩があっても他人に容易に内容を知られないようにすることも広く行われている。

【０００５】

しかしそれでも、通信の盗聴や暗号文の解読や盗み見などによりパスワードを盗まれることがあり、完全に安全なものとは成り得ない。また、パスワードを複雑にするほど利用者自身がそれを正確に記憶しておくことが困難になる欠点がある。さらに本質的には、どれほど複雑なデータであっても、それがデジタルデータとして蓄えられた瞬間から何らかの手段により複製することが可能になるという性質がある。

【０００６】

なりすましを防止し本人であることを確実に認証するため、指紋や声紋など、いわゆる生物学的特徴を表す情報を用いてユーザ認証する方法も検討されている。しかし、一般に生物学的特徴データは情報量が大きいため認証を必要とする利用現場とユーザの生物的情報を蓄積している認証局の間で膨大な通信量を交換しなければならない。したがって、通信路の輻輳や通信時間の長大化のため特殊な環境における場合以外には実用化することが困難であり、かつそのデータの管理場所と管理方法に問題があった。

【０００７】

【発明が解決しようとする課題】

そこで、本発明が解決しようとする課題は、電子情報交換や電子商取引における個人認証を行うための安全性が高く迅速に結果が得られるユーザ認証システムと、これに用いられるユーザ認証票およびユーザ認証装置を提供することである。

【０００８】

【課題を解決するための手段】

上記課題を解決するため、本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを取得する人証取得装置を設けた認証利用所を備え、認証利用所の認証票読取り装置で読みとったユーザ認証票の記録内容と人証取得装置で取得したユーザの生物学的特徴データを比較することによりユーザ認証することを特徴とする。

【０００９】

また、本発明の第２のユーザ認証システムは、ユーザの生物学的特徴データを取得する情報取込み装置を備えた登録所と、ユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行する認証票発行所と、ユーザの生物学的特徴データを取得する人証取得装置と取得した生物学的特徴データをユーザ認証票に入力する人証情報書込み装置とを設けた認証利用所を備え、ユーザ認証票の演算装置を用いて、記録されている生物学的特徴データの内容と人証取得装置で取得されたユーザの生物学的特徴データを比較することによりユーザ認証票の正当な所有者であることを認証することを特徴とする。

【００１０】

これら本発明のユーザ認証システムは、さらに、認証利用所と情報通信路で接続された少なくとも１個の認証局を備え、ユーザ認証票には登録所において取得したユーザの生物学的特徴データの一部を除いて記録しておき、ユーザ認証票に記録しない部分を認証局に記録しておいて、認証利用所からの照会に応えてユーザ認証票において不足する生物学的特徴データの部分を比較して認証するようにすることが好ましい。

なお、情報通信路を介して相互に交換する情報は暗号化して安全性を保証することが好ましい。

【００１１】

また、２個以上の認証局があって、登録所で取得したユーザの生物学的特徴データのうちユーザ認証票に記録しない部分を分割して記録しておいて、各認証局

毎に認証利用所もしくは他の認証局からの照会に応えて自己の記憶する生物学的特徴データの部分を比較して認証するようにすることがより好ましい。

さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えてもよい。

また、認証局における生物学的特徴データを記録した記憶媒体はユーザ認証システムの情報通信路から切り離せるようになっていることが好ましい。

なお、生物学的特徴データとして筆跡を用いてもよい。

【００１２】

本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データの少なくとも一部を記録したユーザ認証票を使用して、ユーザが入力した生物学的特徴データとユーザ認証票の生物学的特徴データを比較することによりユーザ認証するため、ユーザ自身でなければ認証テストをパスすることができないので、パスワードの窃取によるなりすましを防止できる。

【００１３】

また、デジタルデータ化された生物学的特徴データから元の生物学的特徴データを復元することは極めて難しいばかりか、たとえ復元ができてもその生物学的特徴を他人が複製することはできないため、ユーザ認証の信頼性が極めて高い。

特に、ユーザ認証票に照会用の生物学的特徴データを記録しているため、遠隔の認証局でユーザ認証をしてもらわなくても、認証を必要とする認証利用所において本人であることを直接確認することができる。このため認証局との通信に多大な時間および費用を費やす必要がない。

【００１４】

なお、ユーザ認証は、ユーザ認証票に記録した照会用の生物学的特徴データと認証利用所で入力させたユーザの生物学的特徴データとの対照を認証利用所に設けた論理演算装置で行うこともできるが、ユーザ認証票内にＣＰＵやＲＡＭなど演算機能を備えて、ユーザ認証票を利用しようとするユーザから取得した生物学的特徴データを入力し記録されている情報と対照するようにしても良い。

ＩＣカードなど高度な機能を有するユーザ認証票を活用することにより、認証利用所の負担を軽減し装置コストを低減し、システムとしてより利用しやすいも

のとすることができる。また、このようにユーザ認証票内で情報処理を完結させることにより認証票の外部に認証データが漏洩するのを防いで安全性を向上させることができる。

【００１５】

さらに、認証利用所と情報通信路で接続された認証局にユーザの生物学的特徴データのうちユーザ認証票に記録しない残りの部分を記録しておいて、認証利用所からの照会に応えて生物学的特徴データの部分を比較して認証するようにする場合は、必要情報を分割して記憶しておくので、例えば認証票に記録されたデータから生物学的特徴データを復元しても認証システムを突破することはできないし、認証票から認証に用いるデータを複製することもできない。

また、たとえ認証票の記憶内容を改竄しても認証局における情報が保全されているため他人のなりすましを排除することができる。

あるいはまた、認証局がアタックされた場合にもユーザの所有するユーザ認証票の情報まで改竄することができないため安全である。

なお、情報通信路に流す情報が暗号化されたものであれば、通信路の途中で情報を窃取する者があっても解読しにくい為安全性が向上する。

【００１６】

また、ユーザ認証票と２個以上の認証局でユーザの生物学的特徴データを分割して記録しておいて、ユーザ認証票の情報に基づいたユーザ認証に加えて、各認証局毎に認証利用所もしくは他の認証局からの照会に応えて記憶する生物学的特徴データの部分を比較して認証するようにした場合は、例えば階層的に組織された認証局のユーザ認証を段階的に取得することによりユーザ認証の信頼性をより高くすることができる。

【００１７】

なお、本発明のユーザ認証システムでは、要求される認証信頼性のグレードに従い、ユーザ認証票に記録された情報に基づく認証利用所のみの認証で合否決定することを選択しても、ユーザ認証票には記録されていない情報を加味した１個または複数の認証局における認証を追加してより確実な判定を選択してもよい。

たとえば低額の商品を取引する場合はそれほど慎重にユーザ認証を行う必要が

ないのに対して、高額な商品を扱う場合はより高度な保証が必要であるし、病院のカルテなどのように高度のプライバシーに係わるものを扱う場合は確実に本人の請求であるかを確認する必要がある。

【００１８】

このような認証の安全性に対するレベルは認証利用所や取引対象により予め決めておいてもよく、取引毎に認証利用所で設定してもよい。さらに、取引価額などに伴い自動的に選択して設定できるようにしてもよい。

また、この情報分割方式によれば、たとえ生物学的特徴データの全部を用いてユーザ認証を行う場合でも、大部分はユーザ認証票中の情報を用いて認証利用所で認証を行うため、通信回路を介して交換する情報量は小部分であるから、通信回路容量も小さくてよくまた照会に掛かる時間も少ない。

なお、情報を分割することは、多数のユーザについて情報を集積しておき多数の照会を処理しなければならない認証局における処理能力や記憶容量の要求を抑制する効果もある。

【００１９】

さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認定登録局を備えて、登録所において取得したユーザの生物学的特徴データの全容を記録しておくことにより、何らかの不正使用や異常が起きた位置の判定、あるいは認証票が破損したときの再発行、下位の認証局のデータの補修などに利用することができる。

【００２０】

また、認定登録局における生物学的特徴データを記録した記憶媒体がユーザ認証システムの情報通信路から切り離せるようにしておいて必要なときだけ接続して使用するようにすれば、ハッカーの侵入などにより個人情報が漏洩したり改竄されたりすることを防止することができる。

なお、ユーザ認証票や下位の認証局にはそれぞれ部分的な生物学的特徴データのみを記録し完全な記録を残さないようにすることが安全性を確保するために極めて有効である。

【００２１】

本発明のユーザ認証システムで使用する生物学的特徴データとして筆跡を用いてもよい。筆跡は個人の生物学的特徴をよく表して他人のなりすましが難しく、かつ入力する装置および解析する装置が比較的容易に得られるという利点がある。ユーザを識別するために書いて貰う文字や図形は適当なものでよいが、自己の氏名を表すサインなどは再現性がよいため好ましいのはいうまでもない。

また、利用可能な生物学的特徴データには、この他、指紋や掌紋、声紋、虹彩や網膜のパターン、ＤＮＡ情報などがある。今後もより確実で容易に認識できる生物学的特徴が見出される可能性がある。

【００２２】

なお、ユーザ認証票と認証局で生物学的特徴データを分割して記録する場合に、情報データを物理的に分割して前半部分をユーザ認証票に記録し、後半部分を認証局に記録して照合するようにしてもよく、また、例えば筆跡の形状情報をユーザ認証票に記録し筆圧情報や筆順情報を認証局に記録するなど、情報を階層的にとらえて分割する方法を用いてもよい。

さらに、サインと声紋など複数の生物学的特徴データを別々に記録し、それぞれ異なる種類の情報に基づいて判断することにより信頼性を向上させることも可能である。

【００２３】

なお、生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うように構成しても良い。

正規の生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにすれば、例えば、他人に脅かされて意志に反してサインをせざるを得ない事態に陥った場合にサインのどこかに隠し記号を付け加えると、強要者には素直にサインをしているように見せかけて実は警備会社に通報をするといった仕組みにすることもできる。

【００２４】

なお、システム構築上の選択として、このような場合に人身上の安全を確保するため、扉の開閉や現金の引出など普通に取引が成立しているように見せかけるようにすることも可能である。

勿論、こうした目的に使用する生物学的特徴データは正式なものと同じ種類のものであっても良いし、例えばサインに対して音声データを付加するなど異なる種類のものを複合しても良い。

また、逆に、疑似データに特定の符合データを付加したものを正式な認証用データとしても良い。

【００２５】

なお、上記課題を解決するため、本発明のユーザ認証票は、認識票を識別する信号とユーザの個体を区別する生物学的特徴データの少なくとも一部を記録した読出し可能な記憶領域を備えた記憶媒体からなることを特徴とする。

記憶媒体として、ＲＯＭやＣＤ－ＲＯＭなど読み取り専用の記録媒体を使用してもよいが、記録内容が使用者の生物学的特徴を表す情報であるため改竄の危険が少ないので、取引内容や新たな情報を追加して記録できる書き込み読み取り共に可能な記憶媒体であることも可能である。

【００２６】

特に高い偽造防止機能と大きなデータ容量を有し、インテリジェント機能と暗号システムを搭載したセキュリティ機能が高いＩＣカードを利用することが好ましい。

また、ＣＰＵやＲＡＭを搭載したＩＣカードを用いる場合は、ユーザから取得した生物学的特徴データをカード内に取り込んで、内部に記憶した照会用データと比較してユーザ認証を行うようにすれば、認証利用所の負担を軽減し装置コストを低減することができる。また、外部からユーザ認証票の認証データを読み出せないようにして安全性を向上させることができる。

【００２７】

なお、ＩＣカードを使用することにより複合的な機能を搭載し高度な本人認証機能を有する多目的カードにすることができる。ここで使用するＩＣカードは、外部端子により読み書きする接触式と外部端子によらず非接触で読み書きする非接触式を複合した複合ＩＣカードであってもよい。

本発明のユーザ認証票は、特に情報を分散して用いる場合は、記録内容を改竄しても役に立たないので、より経済的で簡便なフロッピーディスクを使用しても

よい。また、この他にも、ＣＤ－ＲＯＭ、ＤＶＤ、録音テープ、ＭＤ等、書き込み可能な各種の記録媒体が使用できる。

【００２８】

また、上記課題を解決するため、本発明のユーザ認証装置は、ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを取得する人証取得装置と、認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと人証取得装置で取得したユーザの生物学的特徴データを照合して合否を判定する判定装置と、判定結果を出力する表示装置を備えることを特徴とする。

【００２９】

本発明のユーザ認証装置によれば、ユーザ認証票を認証票読取り装置にかけると共に、認証を求められたユーザが人証取得装置を介してユーザ認証票に記録されたものと同じ種類の生物学的特徴データを入力すると、判定装置がユーザ認証票に記録された生物学的特徴データと人証取得装置で取得された生物学的特徴データを照合して合否を判定した結果を表示装置に表示するので、外部と通信をしなくても直ちにユーザ認証票の真正な所有者であるか否かを認知することができる。

【００３０】

なお、ユーザ認証装置にはユーザ登録所に設置される生物学的特徴データ入力装置と同じ種類の人証取得装置を備える必要がある。人証取得装置として手書き図形取り込み機能を有するものを使用することができる。手書き図形取り込み機能を利用して、サインなど予め決めた任意の手書き図形をデジタルデータとして入力すれば、ユーザ認証票の生物学的特徴データと比較することが容易に可能となる。

【００３１】

さらに、本発明のユーザ認証装置は外部の認証局と通信できる通信装置を備え、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し合否の判定結果を受け取り、表示装置を介して判定結果を表示するようになっていることが好ましい。

外部の認証局と接続して認証データを階層的に扱うことにより、悪意を持つ侵害者のアクセスや改竄を防止し、より安全性の高い認証能力を備えることが可能となる。

【００３２】

【発明の実施の形態】

以下、図面を参照して本発明の詳細を実施例に基づいて説明する。

図１は本発明のユーザ認証システムの１実施例を示すブロック図、図２は本実施例に使用するユーザ認証装置の例を示す斜視図、図３はユーザ認証装置のブロック図、図４は本実施例に使用するユーザ認証票の例を示すブロック図、図５は本実施例におけるユーザ認証票を発行する手順例を示す流れ図、図６は利用所における認証の手順例を示す流れ図である。

【００３３】

【実施例１】

本実施例のユーザ認証システムは、図１にあるように、認定登録局、認証局および認証利用所からなる階層構造を有する。

認定登録局（ＰＲＡ）１は認証ネットワーク全体を統括するもので、ライセンシーとしての複数の中間認証局（ＰＣＡ）２に一部の権限を与える証明書を発行し、権限を授けられた中間認証局がサブライセンシーとしての複数の末端認証局（ＣＡ）３に一部の権限を与える証明書を発行する。

【００３４】

末端認証局（ＣＡ）３が、ユーザ認証を利用するクライアントとなる認証利用所（ＴＭ）４とクライアントのサービスを利用しようとするユーザ８を仲介する機関となる。なお、以下の説明において各種サービスの利用を取引と表現する場合がある。

なお、認定登録局（ＰＲＡ）１は装置から切り離すことができる記憶装置１１を備え、中間認証局（ＰＣＡ）２と末端認証局（ＣＡ）３は装置に常時接続されている記憶装置２１、３１を備えている。

【００３５】

これらの機関はそれぞれ専用回線や公衆回線により接続されていて、随時情報

の交換ができるようになっている。なお、イントラネット網やインターネット網を利用した連結によってもよい。これら通信回線を用いて情報を交換するときは公開鍵や共通鍵を用いた暗号化処理を行うことにより安全を確保するようにすることが好ましい。

なお、中間認証局（ＰＣＡ）はユーザ認証システムを構築する上で省略が可能である。また、中間認証局（ＰＣＡ）を多段に備えて階層の深さが３段より大きくなっていてもよい。

なお、認定登録局（ＰＲＡ）、中間認証局（ＰＣＡ）、末端認証局（ＣＡ）などの機能は相互に合体した機関が実行するようにしても良いことは言うまでもない。

【００３６】

末端認証局（ＣＡ）は、一般には、行政機関、医療機関、特定企業、共同住宅、商店街（モール）など、対象を限った領域についての権限を認定登録局（ＰＲＡ）や上位の認証局（ＰＣＡ）から授与されている。

末端認証局（ＣＡ）３には、この権限を有する領域に属しユーザ認証を利用する認証利用所（ＴＭ）４が接続されている。

【００３７】

認証利用所（ＴＭ）４に該当するものには、役所の各窓口、病院の各科受付や薬局受付、研究所や部課室の扉、保護を必要とするデータベースにアクセスする情報機器、マンション入口や個室の扉、室内ユーティリティの遠隔操作装置、会員制クラブの施設、モールの各店舗やデパートなど大型小売店の支払窓口、銀行など金融機関の窓口や自動支払機など、各種のものがある。

特にダイレクトマーケティングにおけるユーザ認証は今後さらに重要な課題となり、各ユーザ８の自宅に認証利用所４を設置する状況も考えられる。

【００３８】

末端認証局（ＣＡ）３は、認証利用所（ＴＭ）４を利用しようとするユーザ８を対象として登録の受付をする権限をユーザ登録所（ＲＧ）５に与え、また認証票発行所（ＩＳ）６にユーザ認証票７の発行を行う権限を与える。

【００３９】

ユーザ登録所（ＲＧ）５には、生物学的特徴を取得する入力装置５１が備えられている。本実施例ではタブレットとペンから成るオンライン手書き図形入力装置を利用している。オンライン手書き図形入力装置から筆跡を入力すると、筆記過程の情報を一緒に取り込んで図形認識することができるので、例えば文字を入力したときにも筆画それぞれがどういう方向にどの順序でかかれたかの情報なども容易に取得できる。

【００４０】

また、生物学的特徴をとらえる手段として声紋を利用する場合はマイクロホン５２を装備して音声を入力する。なお、指紋や掌紋を取り込む装置や、瞳を観察して虹彩や網膜パターンを取り込む装置を備えてもよい。

これら人証手段を複数併用することにより、人証をより確実にすることもできる。

【００４１】

認証票発行所（ＩＳ）６には認証票発行装置６１が設置されている。認証票発行装置６１は、ユーザ認証票７に人定に用いられる情報を書き込んでユーザ８に給付する。本実施例におけるユーザ認証システムでは、ユーザ認証票をＩＣカードで構成したが、書き込み読み出し可能な記録媒体であればよく、ＣＤ－ＲＯＭ、フロッピーディスクや磁気カードなど磁気記録媒体、あるいは光磁気記録媒体等、他の電子記録媒体を使用することもできる。

【００４２】

認証利用所（ＴＭ）４には、ユーザ８が持っているユーザ認証票７の真正を検査しユーザ８の認証を行うユーザ認証装置４１が設けられている。

図２と図３はユーザ認証装置４１の１構成例を示す図面である。

ユーザ認証装置４１の上面には、認証票７を挿入するスロットがあって挿入された認証票７の記憶領域と情報をやり取りする入出力装置４０１と、取引に要求される認証の深さを指定する認証レベル指定装置４０２と、ユーザの生物学的特徴データを取得する人証入力装置４０３と、認証結果を表示する認証表示装置４０４が配置されている。

【００４３】

なお、人証入力装置４０３は、ユーザ登録所（ＲＧ）５で用いられる生物学的特徴入力装置５１と同じものである。従って、ユーザ認証に声紋を併用する場合には、認証利用所（ＴＭ）４のユーザ認証装置４１にもマイクロホン４２を付設する必要があることはいうまでもない。このように人証入力装置４０３は、利用するユーザの生物学的情報データの種類に従ってそれを取得するために適合する入力装置を備えている。

【００４４】

また、ユーザ認証装置４１の内部には、これら装置を有機的に結合してユーザ認証を行う電子回路４１０が内蔵されている。

この電子回路４１０は、認証票読取り書込み制御装置４１１と人証情報変換装置４１２と判定装置４１３と通信装置４１４から構成されている。

認証票読取り書込み制御装置４１１は、入出力装置４０１を介して認証票の記録内容を読み取り暗号化されたデジタルデータを復号化しまた認証票に取引結果を記憶させる機能を備えている。

【００４５】

また、人証情報変換装置４１２は、人証入力装置４０３で取り込んだ生物学的特徴データをデジタルデータに変換する。

判定装置４１３は、認証票読取り書込み制御装置４１１と人証情報変換装置４１２と認証レベル指定装置４０２の出力情報を取り込み、必要とされる認証レベルに従って通信装置４１４を介して認証局とやり取りした情報を加味してユーザの個人認証を行い、結果を認証表示装置４０４に表示させる。

【００４６】

ユーザ認証が行われて取引が成立すると取引結果が取引内容入力装置４２０から入力され、その内容は取引表示装置４２１に表示されるので、ユーザ８もこれを確認することができる。また、取引の内容は記憶装置４２２に記録される。

なお、判定装置４１３がユーザ認証結果を自動的に取引内容入力装置４２０に送り、取引の受入あるいは拒否ができるようにしてもよい。

【００４７】

さらに、取引内容入力装置４２０から取引情報を入力してユーザ認証票７に取

引内容や取引履歴を記録するようにしてもよい。

例えばユーザ認証票７を決済分野に使用する場合は取引日と購入商品名と価額を記録しておけば支払い時における対照確認が容易になる。また行政サービス用の認証票では健康保険証や運転免許証、医療情報あるいは住民基本台帳などの証明書類をユーザ認証票７の中に受領して保存するようにすることもできる。

また、ユーザ認証票７に記録された内容を閲覧するときにユーザ認証を条件とすることにより本人以外のアクセスを排除して、個人のプライバシーを保護することができる。

【００４８】

なお、正しい認証に用いるための生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにしてもよい。例えば、強盗や脅迫者などに脅かされて意志に反してサインをせざるを得ない事態に陥った場合に、正規のサインに何気なく隠し記号を付け加えると、扉の開閉や現金の引出など普通に取引が成立するが、同時に警備会社にも通報が行っていて、利用者の安全が確保された状態になったところで犯人を逮捕するなど、適当な処置を執るようにする仕組みを持たせるようなこともできる。

こうした目的に使用する生物学的特徴データとして、例えばサインすると同時に軽く２回咳払いするなど、異なる種類のものを複合して用いても良い。

【００４９】

図４は、ＩＣカードを使用したユーザ認証票の内部構成を示すブロック図である。

本実施例で用いられるユーザ認証票７は、複数の発行者が共同で共用端末を設置し相互解放するための便宜を考慮して、接続端子７１を介して電気信号を伝達する接触型と、カード内の電極７３と認証票読取り書込み制御装置内の電極が接触しないで静電結合や電磁誘導などにより通信する非接触型との両方を備えた複合型ＩＣカードを採用するが、いずれか一方の方式を設備したものであってもよい。

【００５０】

接続端子７１には接続回路７２、非接触電極７３には通信制御回路７４が接続

されていて、内蔵するメモリーと連結されている。

ユーザ認証票７は、ランダムアクセスメモリＲＡＭ７６と読み出し専用メモリＲＯＭ７７と電気的に書込み可能なプログラム可能読取り専用メモリＰＲＯＭ７８と電気的に消去可能なプログラム可能読取り専用メモリＥＥＰＲＯＭ７９からなるメモリーとＣＰＵ７５を備えていて、相互間はバスにより接続されている。

接続回路７２と通信制御回路７４とＣＰＵ７５およびメモリーは１個のＩＣチップに収容することができる。

【００５１】

認証票読取り書込み制御装置４１１は、ユーザ認証票７が挿入されると接続端子７１から接続回路７２を介し、または非接触電極７３から通信制御回路７４を介して、ユーザ認証票７のメモリーにアクセスすることができる。

ＰＲＯＭ７８には認証票の真正性を検査するために使用するカード認証データや証明を受けてユーザ認証票を発行した発行者を明らかにするＩＤなどが格納され、一旦書き込んだデータは書き換えることができない。

ＥＥＰＲＯＭ７９にはユーザの認証に用いる生物学的特徴データや認証票を用いた取引の記録が格納される。またＲＯＭ７７にはＣＰＵ７５を制御して、暗号化や復号化、データ入出力の管制、ユーザ認証装置４１の真正性検査などを行うプログラムが格納されている。ＲＡＭ７６は外部から取り込むデータや演算過程で必要となるデータを一時保持する機能を有する。

【００５２】

ユーザ認証票７は認定登録局１でシステムに使用される適正なカードであることが保証できる正しいカード認定情報をＰＲＯＭ７８に書き込んだ状態で各認証票発行所６に配布されている。従って、認証票発行所６は認定登録局１からの指示に基づいてユーザの生物学的特徴データの一部をＥＥＰＲＯＭ７９に書き込めばよい。カードの改竄を認めないようにするために、認証票発行装置はＰＲＯＭ７８の書き換え機能を備えないようにしても良い。

ただし、本実施例における認証票のメモリー配分は上記に限られず、例えば本人認証を行うための生物学的特徴データをＰＲＯＭ７８あるいはＲＡＭ７６に記録しても良い。

【００５３】

図５を用いてユーザ認証票を発行する手順の１例を説明する。

ユーザ登録所５は、その管轄領域内の認証使用所４のサービスを受けることを欲するユーザ８から登録申請を受け付ける（Ｓ１１）。この時ユーザ登録所５は必要に応じてユーザ８の資格審査に用いる情報を聴取するとともに、ユーザ個人の生物学的特徴を表す情報を取得する（Ｓ１２）。ここで利用する生物学的特徴はユーザ個体に特有であって、他人が模倣や変装などによりそのユーザになりすまそうとしても見破ることができるような性質を有するものが選択される。

【００５４】

本実施例では、筆跡を用いて識別するようにしている。入力する図形は任意でよいが、ユーザ８が入力する度に異なるのは認証を行う上で具合が悪いので、普通は、再現性を保証するため自己の氏名を表すサインを入力させるのが好ましい。なお、複数の生物学的特徴を用いると認証の安全性が向上するため、補助的にマイクロホン４２を用いて声紋も取得できるようにしてある。

ユーザ登録所５で採取された申込人の資格情報と生物学的特徴データは認定登録局１に伝送される（Ｓ１３）。

【００５５】

認定登録局１は、ユーザ登録所５から受け取った情報に基づいて資格審査をし、合格した者に対して認証票の発行を許可する（Ｓ１４）。資格条件は認証を利用する対象に従って決まるので、実際にユーザを受入れる末端認証局３で審査するようにしてもよい。

認定登録局１は、登録ユーザ８の生物学的特徴データを所定の割合に従って階層的に分割し、ユーザ認証票７と各段階の認証局２、３に分配する部分を決定して各所に配布する（Ｓ１５）。

【００５６】

認定登録局１で各所に分配された生物学的特徴データは、認証利用所４の要求する認証精度に基づいてアクセスするものであり、最も低度の信頼性で足りる場合は認証利用所４の認証装置４１で対照した結果だけで認証できるようにし、中度の信頼性を要求するときは末端認証局３に格納された情報を加味してユーザ認

証し、最も高度の保証を要求する場合は分散格納された全ての生物学的特徴データを統合して判定するようにする。

【００５７】

本発明のユーザ認証システムでは、生物学的特徴データは初めに認証利用所４で真正性を検査して合格したときだけ上位機関の認証を請求できるように構成する。上位の認証機関ではユーザ認証票にない部分の情報を用いた認証を行う。

従って、ユーザ認証票７には最小限ユーザ８が入力する生物学的特徴データと対比することによりある程度の確度で真正ユーザであることが判断できる情報を配分しておかなければならない。

【００５８】

本実施例では約６０％の情報をユーザ認証票７に分配し、末端認証局３に３０％の情報、中間認証局２に残りの１０％の情報を分配することとした。このように級数的に情報量を減少させることで、より多数の認証請求が集まる上位機関の記憶容量を節約し、かつ認証に要する時間負荷を減少させる効果が生じ、システム全体としての情報保護性能の向上を図ることができる。

【００５９】

なお、より高度な保証を要請されたときに上位の機関に送達する情報が過大にならないためには、ユーザ認証票７に保持する生物学的特徴データの割合がある程度大きい方が好ましい。

しかし、ユーザ認証票７に与える情報の比率が過大になるとユーザ認証の信頼性が低下する。

従って、生物学的特徴データの分配に当たっては、接続するユーザ数や要求される認証の安全性などを勘案し、実際の条件に適合した適切な分割割合を定める必要がある。

【００６０】

情報の分割方法は、デジタル情報化されたデータを所定の割合で物理的に分割する方法であってもよいが、また筆跡のように描き終わった形状に関する情報と描いている途中の筆勢に関する情報、さらに筆順などの情報というように段階を追った情報として分割してもよい。例えば、声紋を周波数帯に分割したり指紋を

指毎に分けてそれぞれに記録して利用するなど、生物学的特徴は、いずれも適当に分割して利用することができる。

なお、筆跡と声紋など複数の特徴を取得して異なる種類ごとに分割して用いてもよい。

【００６１】

認定登録局１は、認証票とユーザに関する情報を磁気テープやＣＤ－ＲＯＭ、光磁気ディスク、ＤＶＤ、あるいはリムーバブルハードディスクなど、装置から切り離すことができる大容量の記憶手段１１に記録して保存し（Ｓ１６）、下位機関から要請があったときに係員が再生装置に装着して登録された情報を照会するようにする。

認証登録局１では、取り外し可能な記録装置１１を用いて、情報記録媒体１１は不要時には外部の通信回路網から切り離して保管するので、外部からの侵襲や改竄を防止することができる。

【００６２】

認証局２、３に配布された個人の生物学的特徴データはそれぞれに付属する記憶装置２１、３１に格納され必要に応じて随時読み出して利用する。

認証票発行所６は、認証票毎に決められたカード認証暗号が記録されているユーザ認証票７に認定登録局１から分配を受けた登録申込人の生物学的特徴データを記録してユーザ８に支給する（Ｓ１７）。

【００６３】

なお、１個の末端認証局（ＣＡ）３に複数のユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６を備えてもよい。

ユーザ８はユーザ登録所５に出頭して実際に自身の生物学的特徴を入力しなければならないので、発行されたユーザ認証票７を受け取る認証票発行所６がユーザ登録所５と同じ場所に設置されているとユーザ８の便宜のために好ましい。

【００６４】

なお、ユーザ８の人定のため信頼がおける人物の立会を条件とするようにしてもよい。ただし、初めから他人になりすましている場合を完全に排除することはどの様な機構を用いても困難である。

また、登録するユーザが申告した事実を確認するためには、登録手続と同時に認証票を発行する方式でなく、後に住所に郵送する方式を採用してもよい。

なお、認定登録局（ＰＲＡ）１がユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６を備えるようにしてもよい。

さらに、ユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６の機能を備えた携帯用端末を持った発行者が任意の場所において登録発行手続をすることも可能である。このような携帯用端末の利用は認定登録局（ＰＲＡ）から正規の資格認定を受けた者しか認めないようにする必要があり、ここでも発行者としての厳重な認証を受けて始めて操作できるように構成されている。

【００６５】

次に、図６を用いて、認証利用所４においてユーザ認証票７によりユーザ認証をする手順の１例を説明する。

ユーザ８がユーザ認証票７を提出して認証利用所４に取引を申し出ると、認証利用所４はその認証票７を認証装置４１のカードスロット（入出力装置）４０１に挿入して認証用の情報を読み取る。認証用の情報にはカードの真正性を確認するための情報とユーザ認証のための生物学的特徴データとが含まれる。

【００６６】

認証利用所４は初めにカードの認証を行う（Ｓ２１）。カードの認証は、ユーザ認証票７が認証利用所４が使用するユーザ認証システムに適応する真正なものであり正当な所持者が誰であるかを確認することである。対応しない認証票を使用している場合は初めから取引を受け付けない。

なお、逆にユーザ認証票７が不正にアクセスされていないことを確認するために、ユーザ認証票７中のプログラムにより認証装置４１が自身の認証票と対応するものであるかを検証して、正しい認証装置でない場合は記憶内容の開示を拒絶する仕組みを備えてもよい。

【００６７】

カード認証で合格したときには、ユーザ８にタブレット（人証入力装置）４０３上にサインを書いて貰うなど、ユーザ認証票７を取得したときに用いたものと同じ生物学的特徴を表示することを求める（Ｓ２２）。

そして、タブレット４０３から入力した生物学的特徴データをユーザ認証票７に記録されていた例えば６０％の生物学的特徴データと照合して、窓口のユーザ８がユーザ認証票７の真正な所持者か否かを判定する（Ｓ２３）。ユーザ認証結果は表示装置４０４に表示する（Ｓ２４）。

【００６８】

認証利用所４におけるユーザ認証の合否に従い手順が異なる（Ｓ２５）。ユーザ認証が否定されたときは認証利用所４は取引を拒絶する（Ｓ３３）。ユーザ認証に合格したときはさらに上位の認証機関にオンライン認証を求めるべきか否かを調べる（Ｓ２６）。オンライン認証を必要としない場合は直ちに取引の申し出を受け入れてよい（Ｓ３２）。

オンライン認証の要求の有無や深さの要求度は取引毎に認証レベル指定装置４０２からオペレータやユーザ８が入力してもよいが、取引の性格や取引金額の多寡に基づいて自動的に設定されるようにしてもよい。

【００６９】

オンライン認証を必要とする場合は、認証レベルの要求と共にユーザ認証票７の情報と人証入力装置４０３で取得した人証情報とを末端認証局３に送付する（Ｓ２７）。送付する人証情報は、認証利用所４で利用した部分を除外した例えば４０％の部分でよいから、認証利用所４と末端認証局３の間で交換する情報量を縮減することができる。

【００７０】

オンライン認証の要否は、取引の性格に従った認証の安全性に対する要求水準により決められる。換金性の高い商品や高額商品の取引とか個人の秘密情報の開示にはより安全な認証が必要とされるので、上位機関のユーザ認証が求められることになる。

また、認証利用所４の性格によってオンライン認証の深さが指定される場合もある。病院の窓口などではプライバシーの保護と正確な治療行為を保証するため高度な本人認証が必要とされる場合が多い。なお、通信回線を使った在宅診療などでは確実に本人のデータであることを確認するため、上位の認証局までユーザ認証を求めるようにすることが好ましい。

【００７１】

末端認証局３では記憶装置３１に記録されているユーザ８の固有の人証情報と照合して（Ｓ２８）、認証結果を認証利用所４に回付する（Ｓ２９）。

末端認証局３にはユーザの人証情報の３０％しか記録されていないので、ここにおけるユーザ認証だけでは不足する場合は、さらに上位の中間認証局２にユーザ認証を求める。中間認証局２には各ユーザについて１０％の生物学的特徴データを記録してあるので、認証利用所４で取得した人証情報のうち中間認証局２で使用する部分は１０％になり、末端認証局３から中間認証局２に送付すべき情報量はさらに大幅に減少する。

中間認証局２で行ったユーザ認証結果は末端認証局３を介して認証利用所４に返る。

【００７２】

各所のユーザ認証結果は認証利用所４で総合されてユーザ認証装置４１の認証表示装置４０４に表示される。ユーザ認証が合格の場合は取引を受け入れ（Ｓ３２）、不合格の場合は取引を拒否（Ｓ３３）することになる（Ｓ３１）。

また、ユーザ認証が否定されたときは改竄やなりすましなど何らかの不正行為の可能性もあるので、その情報を認定登録局１まで送付して問題の在処を確認して原因の解析を行うことが好ましい。

【００７３】

認定登録局１には外部から侵入したり改竄することが困難な記録が保管されているので、認証利用所４における入力データと対比することにより、異常がユーザ認証票７にあるのか、末端認証局３にあるのか、あるいは中間認証局２にあるのかが明確になる。

ユーザ認証票７の内容とユーザ８が入力した情報の間に齟齬がある場合は盗難や拾得により真正でないユーザが使用している場合やユーザ認証票のデータが不当なアクセスにより書き替えられた場合が考えられる。

【００７４】

【実施例２】

本実施例のユーザ認証システムが第１の実施例と異なる点は、認証利用所に設

けた論理演算装置でユーザ認証票に記録した生物学的特徴データと人証取得装置で入力させたユーザの生物学的特徴データとを対照して行う代わりに、ユーザ認証票内の演算機能によりユーザの生物学的特徴データと記録された人証情報とを対照するようにした点のみであるので、ここでは、第１実施例の説明に使用した図面を用いて第１実施例と異なる部分についてのみ説明する。

【００７５】

ユーザ認証票７として使用するＩＣカードには、ＣＰＵ７５やＲＡＭ７６などを搭載して一定の演算機能を持たせることができる。

本実施例のシステムでは、認証利用所４でサービスを利用しようとするユーザ８がユーザ認証装置４１を用いてユーザの生物学的情報データを入力すると、この生物学的情報データを所定の処理をしてデジタル処理しやすい形態に変換した上でユーザ認証票７に送付する。

【００７６】

ユーザ認証票７は入力された情報データを一旦ＲＡＭ７６に記憶し、ＣＰＵ７５でこの情報データとＥＥＰＲＯＭ７９に記録されている正当ユーザの生物学的情報データを読み出しながら両者を突き合わせて比較する。その結果、両者が許容範囲内で類似していてサービスを利用しようとする人間がユーザ認証票７の正当な所有者ということが認証できれば認証利用所４に合格を通知し、この認証にパスしなければ拒絶を通知する。

【００７７】

認証利用所４は、ユーザ認証票７のユーザ認証結果に満足すれば利用者８に所望のサービスを提供する。また、さらに慎重なユーザ認証を必要とする場合は末端認証局３や中間認証局２に照会を行って、その結果と合わせて判定する。なお、認証利用所４が末端認証局３を兼ねていても良いことは言うまでもない。

各所に生物学的情報データを配布する割合は任意であるが、第１実施例で例示したと同様に下位水準の認証に用いるものほど大きな割合にすると通信における負担が軽くなりシステムの運用上有利で、ユーザ認証票７における割合を６０％以上にすることが好ましい。

【００７８】

本実施例では、高機能ＩＣカードからなるユーザ認証票７を活用することによりユーザ認証装置４１の演算上の負担を軽減し装置のコストを低減できることから、認証利用所４の機能を調えるのに必要とされる費用が小さくなるので、システムに参加するための障壁が低くなりより利用しやすくすることができる。

また、ユーザ認証票内で情報処理を完結させるので、認証票のメモリに外部からアクセスできない読み出し不可領域を設けて、ここに認証データなど重要な情報を記録して漏洩を防ぐようにして安全性をより向上させることができる。

【００７９】

【発明の効果】

以上詳細に説明した通り、本発明のユーザ認証システムを用いれば、認証利用所において直接にユーザが入力する人証情報と認証票内の生物学的特徴データを照合し、より高度の保証を欲するときに上位の認証局に人証情報の一部を伝送してユーザ認証をするため、情報処理の大部分を認証利用所で行って通信回路に大きな負荷をかけることなく、安全性の要求水準に対応したユーザ認証を得ることができる。また、人証情報を分割することにより侵襲に対して極めて強いユーザ認証システムの構築が可能となる。

【図面の簡単な説明】

【図１】

本発明の実施例のユーザ認証システムを示すブロック図である。

【図２】

本実施例に用いられるユーザ認証装置の例を示す斜視図である。

【図３】

本実施例におけるユーザ認証装置の回路ブロック図である。

【図４】

本実施例に使用するユーザ認証票の構成例を示すブロック図である。

【図５】

本実施例におけるユーザ認証票を発行する手順例を示す流れ図である。

【図６】

本実施例における利用所における認証の手順例を示す流れ図である。

【符号の説明】

１　認定登録局

１１　切離し可能な記憶装置

２　中間認証局

２１　記憶装置

３　末端認証局

３１　記憶装置

４　認証利用所

４１　ユーザ認証装置

５　ユーザ登録所

５１　人証入力装置

５２　マイクロホン

６　認証票発行所

６１　認証票発行装置

７　ユーザ認証票

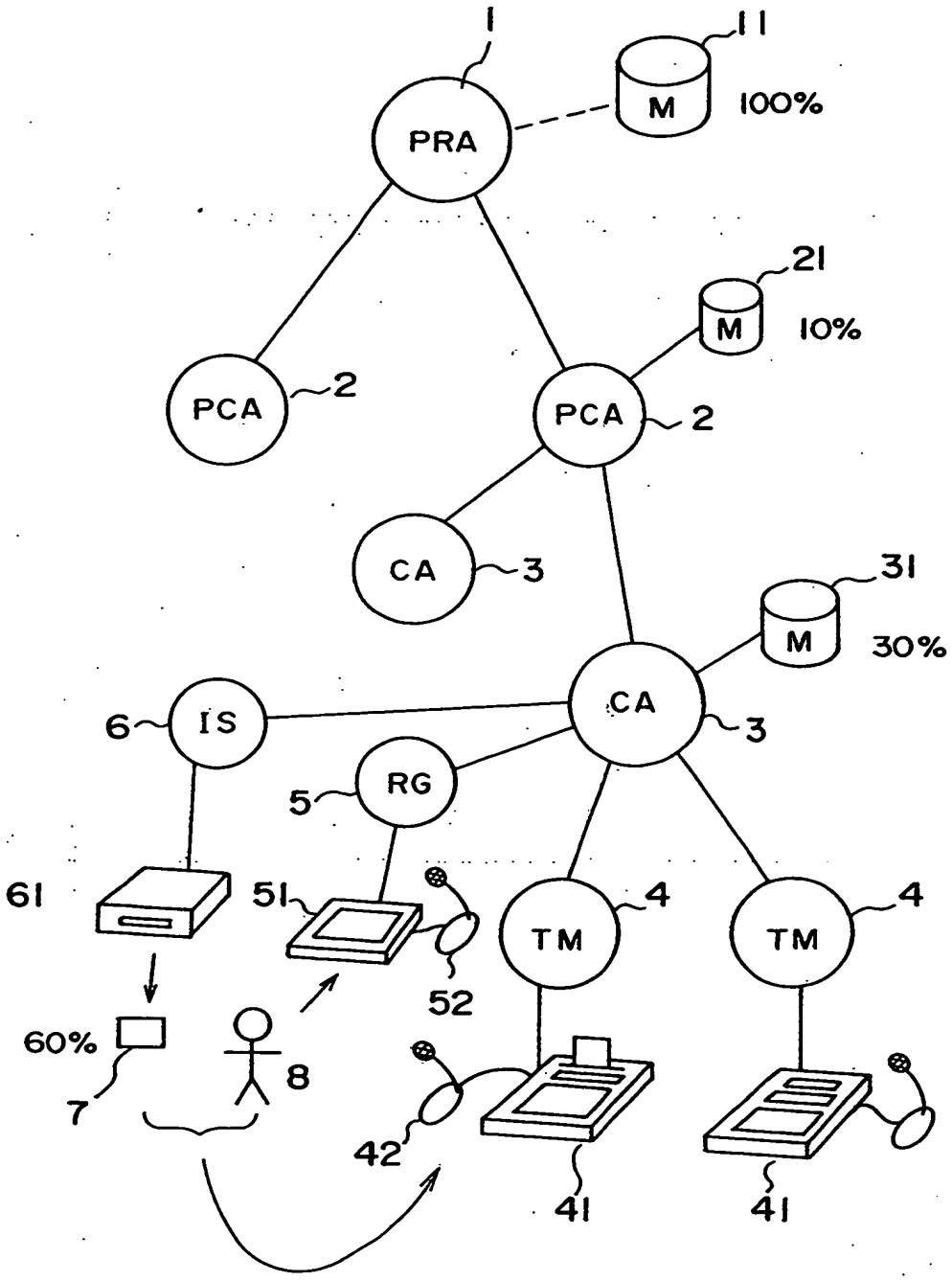
７１　接続端子

７３　非接触電極

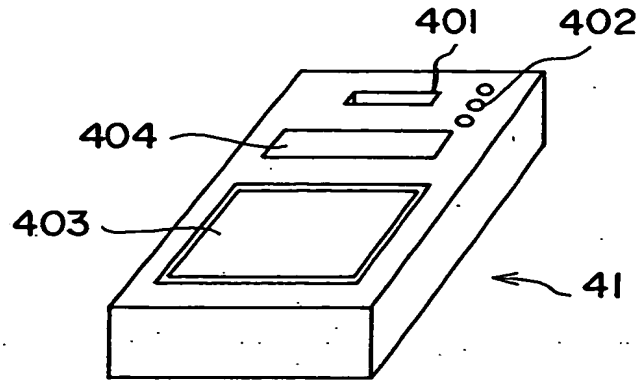
８　ユーザ

【書類名】　図面

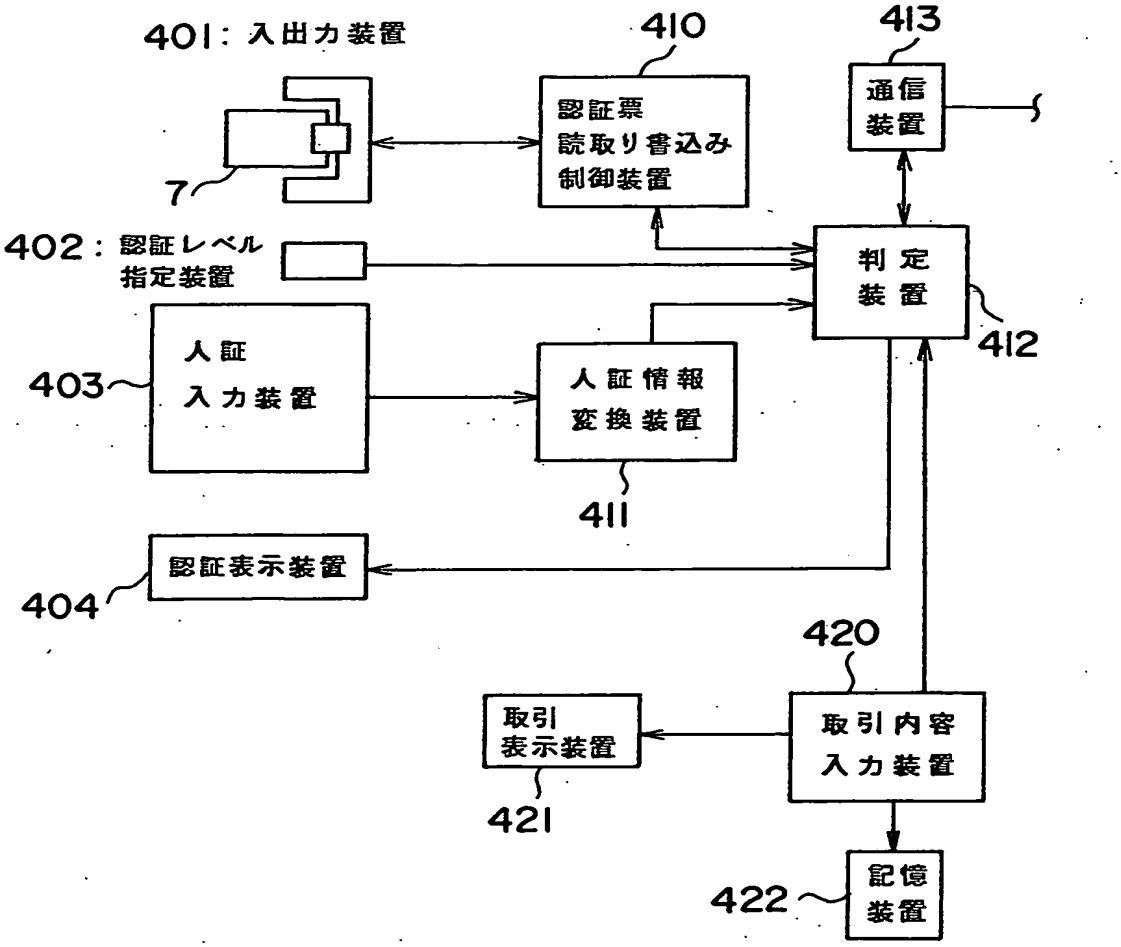
【図１】


1
11
M
100%
PRA
21
M
10%
PCA
2
PCA
2
CA
3
31
M
30%
CA
3
6
IS
5
RG
61
51
52
TM
4
TM
4
60%
7
8
42
41
41

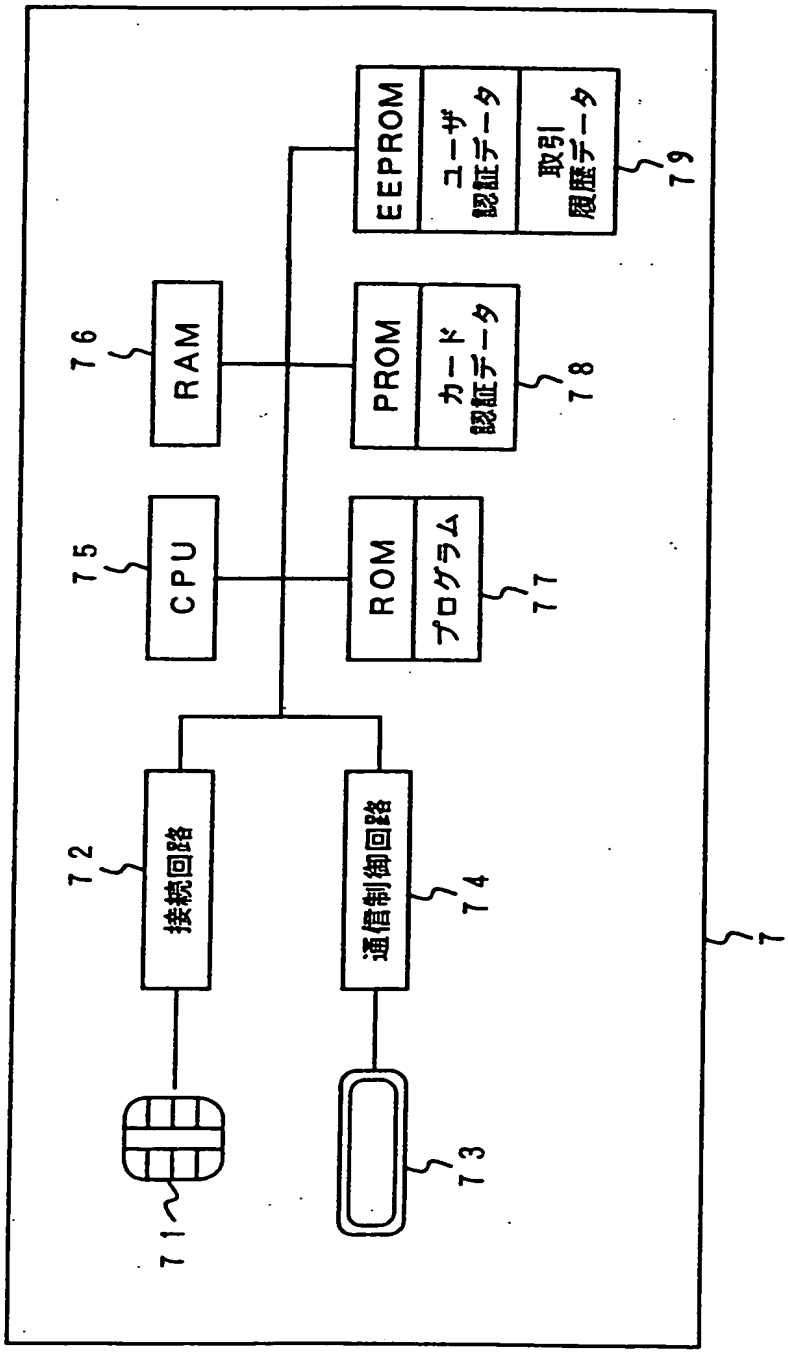
【図２】


401
402
404
403
41

【図３】

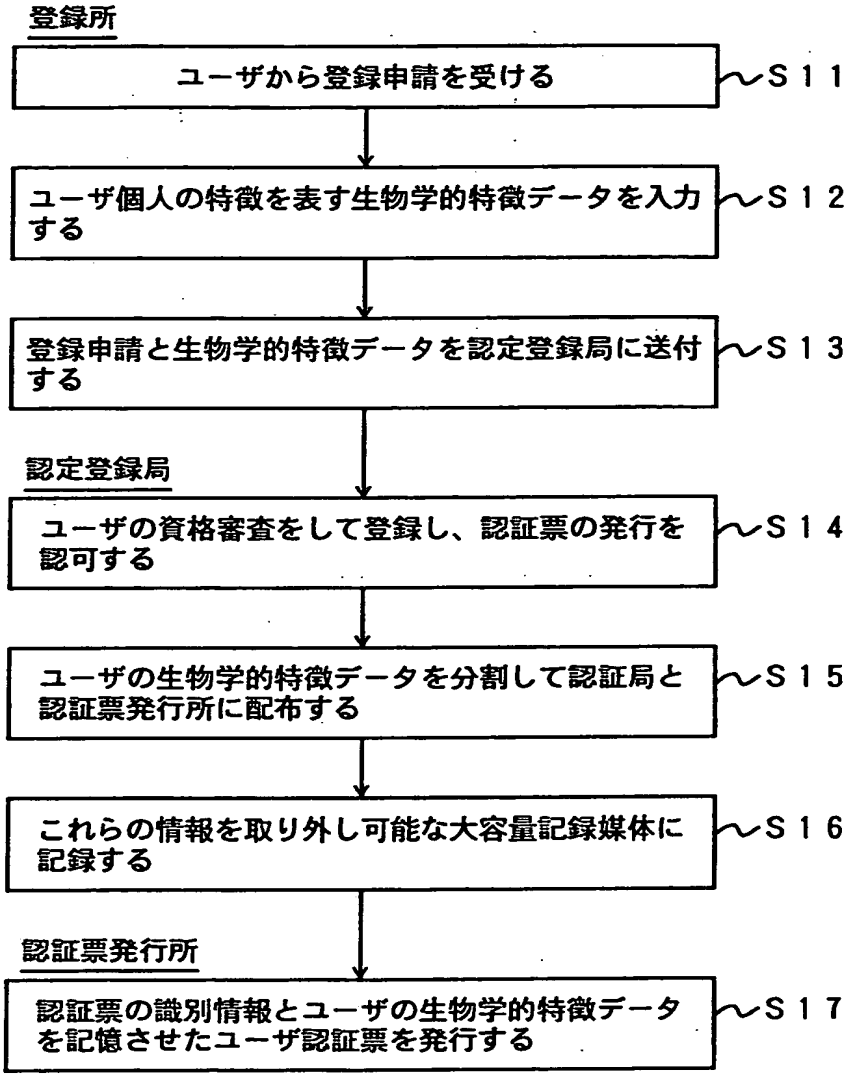

401：入出力装置
410
413
認証票
読取り書込み
制御装置
通信
装置
7
402：認証レベル
指定装置
判定
装置
412
人証
入力装置
403
人証情報
変換装置
411
認証表示装置
404
420
取引
表示装置
421
取引内容
入力装置
記憶
装置
422

【図４】


EEPROM
ユーザ認証データ
取引履歴データ
79
RAM
76
PROM
カード認証データ
78
CPU
75
ROM
プログラム
77
接続回路
72
通信制御回路
74
7
71
73

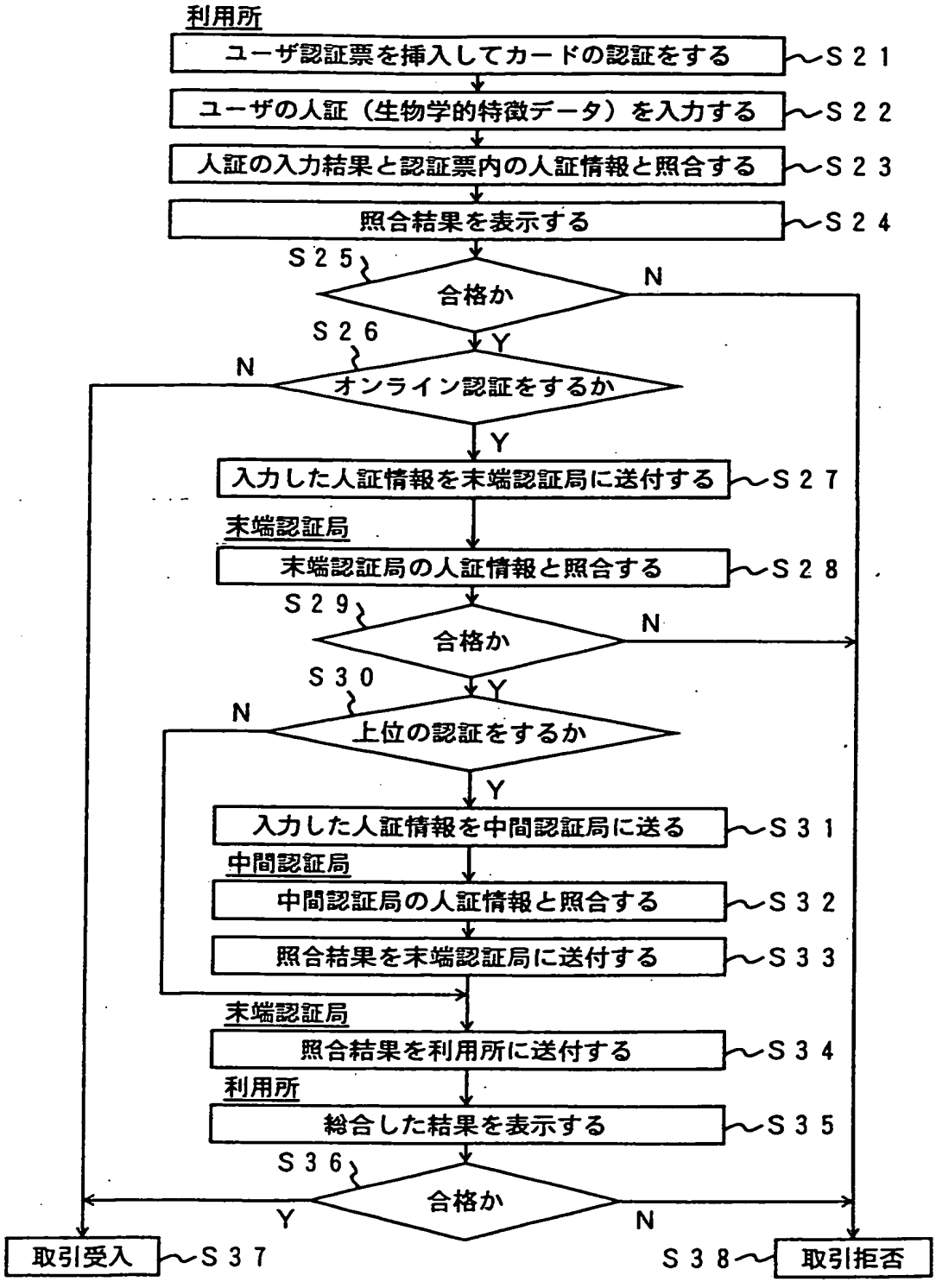
【図５】

ユーザ認証票の発行



【図６】

利用所における認証


利用所
ユーザ認証票を挿入してカードの認証をする
S２１
ユーザの人証（生物学的特徴データ）を入力する
S２２
人証の入力結果と認証票内の人証情報と照合する
S２３
照合結果を表示する
S２４
S２５
合格か
N
Y
S２６
オンライン認証をするか
N
Y
入力した人証情報を末端認証局に送付する
S２７
末端認証局
末端認証局の人証情報と照合する
S２８
S２９
合格か
N
Y
S３０
上位の認証をするか
N
Y
入力した人証情報を中間認証局に送る
S３１
中間認証局
中間認証局の人証情報と照合する
S３２
照合結果を末端認証局に送付する
S３３
末端認証局
照合結果を利用所に送付する
S３４
利用所
総合した結果を表示する
S３５
S３６
合格か
Y
N
取引受入
S３７
S３８
取引拒否

【書類名】　要約書

【要約】

【課題】　安全性が高く迅速に結果が得られるユーザ認証システムと、これに用いられるユーザ認証票およびユーザ認証装置を提供する。

【解決手段】　ユーザ８の個体を区別する筆跡声紋等の生物学的特徴データを取得してその生物学的特徴データの少なくとも一部を記録したユーザ認証票７を発行し、認証票読取り装置４１で読み取ったユーザ認証票７の記録内容と人証取得装置に入力されたユーザの生物学的特徴データを比較することにより認証利用所４で直接にユーザ認証する。また上位の認証局２、３を備え、ユーザの生物学的情報の全てをユーザ認証票７に記録しないで、残った部分を各認証局毎に記録しておいて、認証利用所４の照会に応えて記録した生物学的特徴データの部分を比較して追加認証することにより認証の信頼性を向上させることができる。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【提出日】　平成10年 5月21日
【特許出願人】
　【識別番号】　398035796
　【住所又は居所】　千葉県八千代市勝田台南２丁目１５番２２号
　【氏名又は名称】　保倉　豊
【代理人】　申請人
　【識別番号】　100104341
　【住所又は居所】　東京都千代田区五番町４番地　幸ビル４階　関特許事務所
　【氏名又は名称】　関　正治

出 願 人 履 歴 情 報

識別番号　〔３９８０３５７９６〕

１．変更年月日　１９９８年　５月　７日
［変更理由］　新規登録
住　所　千葉県八千代市勝田台南２丁目１５番２２号
氏　名　保倉　豊